La vidéosurveillance dans l'oeil de la Constitution

Flückiger, Alexandre; Auer, Andreas

How to cite

FLÜCKIGER, Alexandre, AUER, Andreas. La vidéosurveillance dans l'oeil de la Constitution. In: Aktuelle juristische Praxis, 2006, vol. 8, p. 924–942.

This publication URL: https://archive-ouverte.unige.ch/unige:679

DIKE VERLAG AG
CH-8853 LACHEN

AJP/PJA 2006 p. 924-942

La vidéosurveillance dans l'œil de la Constitution

Die Video-Überwachung wird heute öfters und verbreiteter eingesetzt; zugleich erhöht die spektakuläre technologische Entwicklung die daraus für den Rechtsstaat und die Grundfreiheiten resultierenden Risiken. Unter dem Gesichtspunkt der hinreichend bestimmten gesetzlichen Grundlage lässt die einschlägige Bundesgesetzgebung zu wünschen übrig, insbesondere was die Überwachung der Grenzen und des öffentlichen Verkehrs anbelangt. Demgegenüber fehlen in vielen Kantonen gesetzliche Grundlagen überhaupt. Die mit Video-Überwachungen verbundenen Einschränkungen der Freiheiten sind im Übrigen unter verfassungsrechtlichen Gesichtspunkten nur akzeptabel, wenn sie mit praktisch wirksamen Vorkehrungen, welche das Verhältnismässigkeitsprinzip erfordert, verbunden und mit Evaluationen begleitet werden.

Alexandre Flückiger, Professeur à la Faculté de droit de l'Université de Genève
Andreas Auer, Professeur à la Faculté de droit de l'Université de Genève

---

Plan:

1. Introduction

La vidéosurveillance est en plein essor, en Suisse aussi bien qu'à l'étranger. La guerre contre le terrorisme, la lutte contre la criminalité et le relâchement du civisme la rendent, aux yeux de certains, aussi désirable qu'indispensable. Pour d'autres, elle symbolise la marche forcée de nos sociétés vers l'univers sécuritaire et l'avènement, avec plus de vingt ans de retard, de *nineteen eighty-four* . Les fronts se raidissent et le fossé se creuse, pendant que la technologie ne cesse de progresser et que les questions, de nature technique, sociétale et juridique, se multiplient.

La présente contribution a pour but d'examiner les problèmes constitutionnels que soulèvent l'installation et l'exploitation de la vidéosurveillance par les autorités. Elle part de l'espoir que notre ordre constitutionnel soit en mesure de fournir des réponses adéquates à la fois aux autorités qui souhaitent recourir à ce moyen et aux particuliers et organisations qui s'en méfient. Car s'il ne l'était pas, il faillirait à la tâche première des sciences sociales, qui est de poser des jalons permettant à l'Etat et la société de rester en contact, de communiquer, tout en gardant leurs distances.

Le résultat est conforme aux attentes. L'ordre constitutionnel ne condamne pas d'emblée la vidéosurveillance. Mais il la soumet à des sérieuses limites, qui découlent principalement du principe de la légalité et de la garantie des libertés.

2. Le phénomène de la vidéosurveillance et son contexte

2.1. Les différents types de vidéosurveillance

Il y a vidéosurveillance et vidéosurveillance. On peut la qualifier *d'observation*, lorsqu'elle est utilisée pour surveiller un rayon déterminé accessible au public, afin de constater des mouvements ou des phénomènes objectifs, sans traiter des données personnelles. Elle devient *dissuasive*, lorsqu'elle consiste à surveiller ouvertement les lieux publics ou les lieux privés accessibles à tous pour tenter d'empêcher les personnes qui s'y trouvent de commettre des infractions. Elle finit par être *invasive* , lorsqu'elle vise à surveiller secrètement une personne se trouvant ou non sur un lieu accessible au public, soupçonnée de s'adonner à une activité délictuelle et relève alors notamment du droit pénal et du droit policier [1].

Même si, dans la pratique, il n'est pas toujours aisé de les distinguer clairement [2], les trois types de vidéosurveillance ne sont pas soumis au même régime juridique. S'il en est ainsi, c'est que leurs finalités et leur impact sur les droits des personnes surveillées ne sont pas les mêmes. En raison de son but principalement préventif et, par conséquent, de sa portée à la fois personnelle et territoriale très large, la vidéosurveillance dissuasive sera au centre de nos préoccupations. Mais les distinctions ne s'arrêtent pas là.

On parle de *vidéosurveillance simple* lorsque l'appareillage de surveillance est simplement relié à un ou plusieurs écrans de contrôle, qui n'enregistrent ni image, ni son, mais qui permettent d'observer et d'identifier les personnes se trouvant sur les lieux surveillés. C'est un peu comme si un agent de police observait sur place le comportement de ces personnes, de sorte que les caméras vidéo ne représentent finalement qu'un moyen technique pour permettre à un seul agent d'observer simultanément plusieurs lieux.

La *vidéosurveillance informatisée* ouvre d'autres perspectives. Du moment en effet que l'image filmée n'est pas (seulement) visionnée en direct, mais enregistrée, pour être mémorisée, conservée et traitée selon toutes les astuces et techniques que l'informatique met à disposition du surveillant, l'impact sur les personnes est autrement plus grave. L'aggravation résulte de plusieurs causes.

Elle résulte tout d'abord du *facteur temporel*: le comportement enregistré peut être observé et analysé pendant toute la durée de la conservation des données. Elle résulte aussi du *facteur personnel* : les données sont accessibles à plusieurs personnes et peuvent être communiquées très simplement à d'autres instances, ou au public en général, par Internet notamment. Elle découle également de *facteurs géographiques*: en s'étendant constamment, le dispositif de vidéosurveillance peut être mis en réseau permettant de tracer ainsi le déplacement d'un individu, ce qui peut conduire à l'établissement d'un profil de sa personnalité.

L'aggravation résulte enfin et surtout du *facteur technologique*: les progrès en matière d'imagerie numérique modifient radicalement les éléments de fait permettant de qualifier l'intensité de la surveillance. Les caméras en haute définition permettent ainsi de repérer aisément un visage dans une foule. Les technologies en matière de résolution d'image, de zoom, de son, de miniaturisation, de vision nocturne et de suivi rendent possible une surveillance à longue distance, une reconnaissance des détails dans une scène panoramique large, une identification de voix ou de conversations et un traitement en temps réel. On peut penser à la détection automatisée de mouvements ou de comportements hors norme (arrêt d'une voiture, abandon d'une mallette, tentative de suicide le long des voies de métro, corps flottant entre deux eaux dans une piscine [3)], au repérage des traits somatiques ou de la couleur d'un visage, aux dispositifs de reconnaissance thermique, qui permettent de voir parfaitement durant la nuit ou même derrière des murs ou encore aux avions télécommandés (drones), dotés de caméras de haute définition permettant d'identifier des individus.

Les capacités sans cesse croissantes en matière de stockage de l'information numérique et l'aisance de sa gestion n'offrent dorénavant plus aucun point de comparaison avec l'armoire d'archivage des vidéocassettes.

L'avènement de la vidéosurveillance informatisée estompe la pertinence de la distinction entre la vidéosurveillance d'observation et la vidéosurveillance dissuasive surtout. Le phénomène devient ainsi intrusif par définition. On comprend dès lors que la vidéosurveillance informatisée pose des problèmes juridiques particulièrement délicats.

2.2. La vidéosurveillance par les autorités et par les particuliers

Alors que le droit français [4] et le droit allemand [5] réglementent de manière analogue la vidéosurveillance dissuasive des lieux accessibles à tous, indépendamment de leur appartenance publique ou privée, le droit suisse de la protection des données retient une conception différente, qui conduit à un certain morcellement de la problématique. Il distingue en effet la question non pas du point de vue de l'accessibilité publique ou privée des espaces surveillés, mais seulement selon le statut juridique de celui qui institue et effectue la vidéosurveillance. La loi fédérale sur la protection des données, du 19 juin 1992 (LPD) [6], opère ainsi une distinction entre le traitement des données qui est le fait d'organes publics fédéraux (art. 16 à 25) et celui qui est orchestré par des particuliers (art. 12 à 15) [7]. Conséquence de la structure fédérale, cette loi ne s'applique pas à la collecte et au traitement des données personnelles par les autorités cantonales ou communales, qui sont régis par le droit cantonal.

Cette distinction présuppose que les personnes privées soient habilitées à surveiller leur propriété par des caméras en vertu du pouvoir de disposition découlant de leur titre de propriété et dans les limites juridiques de l'exercice de celui-ci, alors que les collectivités publiques et les organes

---

qui agissent en leur nom disposent du domaine public qui leur échoit dans le cadre de leurs compétences propres ou déléguées, ainsi que de la répartition des compétences entre la Confédération et les cantons.

Il en résulte que les autorités, à l'exception de la police [8] et sous réserve d'une infraction pénale, ne sont pas habilitées à exercer une vidéosurveillance en dehors du domaine public et des lieux privés ouverts au public à défaut du consentement du propriétaire ou d'une base légale spécifique [9], en raison de l'atteinte que causerait un tel dispositif à la garantie de la propriété, voire à la liberté économique.

Précisons que les cantons sont habilités à réglementer la vidéosurveillance sur le domaine public et le patrimoine administratif. Dans ce cas, les règles découlant du droit de la protection des données s'appliquent en concours avec les principes régissant le domaine public et le patrimoine administratif.

2.3. La vidéosurveillance du domaine public et du patrimoine administratif

Selon la doctrine et la jurisprudence, le domaine public comprend l'ensemble des choses et des biens qui ne sont pas affectés à une finalité particulière par l'Etat et qui peuvent être utilisés par les particuliers sans intervention des agents publics, en principe d'une manière libre, égale et gratuite: les rues, les places, les ponts, les parcs et les promenades. Par opposition, le patrimoine administratif regroupe les biens immobiliers et mobiliers affectés par l'Etat à une tâche déterminée, comme les écoles, les hôpitaux, les musées, les terrains et stades de sport, etc. [10]

En droit cantonal genevois [11], la notion de domaine public est définie par la loi sur le domaine public du 24 juin 1961 [12], qui se réfère aux voies publiques cantonales et communales selon le régime fixé par la loi sur les routes, au lac et aux cours d'eau dont le régime est fixé par la loi sur les eaux et aux biens qui sont déclarés du domaine public par d'autres lois. Auparavant, le législateur cantonal s'était référé, à propos des parcs, promenades et jardins publics, à la notion de "domaine privé communal", qui désignait en réalité le domaine public [13].

On pourrait être tenté d'établir une distinction entre les emplacements prévus pour la vidéosurveillance qui se situent sur le patrimoine administratif de la collectivité publique - à l'instar des préaux d'école, des stades communaux et des parkings - et les endroits qui font partie du domaine public, comme les rues et les places publiques. La distinction irait dans le sens que la collectivité aurait plus de droits pour installer les caméras sur son patrimoine administratif que sur le domaine public proprement dit.

En réalité, cette distinction n'est pas pertinente. Car si la collectivité publique désire installer et mettre en service un système de vidéosurveillance dans les préaux d'écoles et dans les parkings, ce n'est pas tant pour surveiller les usagers de ces établissements et lieux que sont les élèves, les parents, les enseignants et les conducteurs de véhicules, mais pour prévenir et, le cas échéant, réprimer les déprédations qui peuvent être commises en ces lieux par toute personne [14]. C'est précisément parce que ces endroits sont ouverts au public, tout en permettant de s'abriter du regard des autres, qu'ils sont le théâtre privilégié d'actes de vandalisme, surtout à certaines heures. Il y a donc lieu d'assimiler l'ensemble des emplacements prévus pour la vidéosurveillance au domaine public.

2.4. Les exigences de base de l'ordre constitutionnel

Ainsi circonscrit, le phénomène de la vidéosurveillance par les autorités doit être analysé dans la double perspective de la légalité et de la conformité aux libertés.

En premier lieu, le principe de la légalité (art. 5 al. 1er Cst.) commande que chaque activité étatique trouve sa base dans une loi. Sa finalité principale est le respect de la séparation des pouvoirs, de l'égalité et de l'interdiction de l'arbitraire, ainsi que la garantie d'un ancrage démocratique des actions étatiques. Si la validité du principe de la légalité s'étend aujourd'hui à l'ensemble des actes qui sont imputables à l'Etat, ses exigences varient en fonction de plusieurs critères, parmi lesquels il convient de citer, notamment, l'impact des mesures sur les droits et les obligations des citoyens, leur pertinence pour les matières considérées comme essentielles pour ce qui est des rapports entre les autorités et les particuliers, etc. (art. 164 al. 1er Cst.).

En second lieu et surtout, le recours à la vidéosurveillance étatique doit respecter et réaliser les droits fondamentaux, parmi lesquels, dans ce contexte, les libertés jouent un rôle essentiel. S'il est vrai que la simple garantie constitutionnelle et conventionnelle des libertés n'empêche pas l'Etat de les restreindre, il importe de porter une attention particulière aux conditions que doivent observer ces restrictions. On retrouve ici, dans une perspective spécifique, l'exigence de la légalité, en ce que les atteintes aux libertés qui sont considérées comme graves exigent une base légale formelle, les autres pouvant se contenter d'une

---

base légale matérielle. S'y ajoutent des considérations portant sur la justification des mesures restrictives et, surtout, sur le principe de la proportionnalité.

3. Le dispositif normatif

3.1. Les règles fédérales

3.1.1. Les exigences spécifiques de la LPD

Le principe selon lequel les restrictions graves aux libertés doivent être prévues par une loi formelle vaut bien évidemment également en droit de la protection des données [15]. Ainsi, le législateur fédéral a d'emblée posé la règle selon laquelle les données sensibles, ainsi que les profils de personnalité, ne peuvent en principe être traitées par les organes fédéraux que si une loi au sens formel le prévoit expressément, parce que l'accomplissement d'une tâche étatique l'exige absolument (art. 17 al. 2 LPD) [16]. Le législateur s'est montré sur ce point plutôt sévère en prenant le risque de gêner dans certains cas le bon fonctionnement de l'activité de l'administration puisqu'il n'est pas toujours possible de prévoir toutes les circonstances [17]. Or, les données personnelles recueillies par les systèmes de vidéosurveillance doivent être considérées d'une manière générale comme des données personnelles sensibles. Voir ci-dessous ch. 4.1.3 *i.f.*

L'exigence de la base légale formelle pour le traitement des données sensibles subit deux exceptions. La première vise le cas où le Conseil fédéral autorise leur traitement, considérant que les droits des personnes touchées ne sont pas menacés (art. 17 al. 2 let. b LPD). La seconde porte sur l'hypothèse où la personne concernée a consenti au traitement des données, ou les a rendues accessibles à tout un chacun (art. 17 al. 2 let. b LPD).

C'est cette dernière exception qui mérite une attention particulière. Le simple fait de se promener dans la rue de manière reconnaissable et identifiable et d'entrer ainsi dans le champ de vision d'une caméra n'équivaut pas encore automatiquement à un consentement à ce que ces images soient traitées, ni ne rend ces données accessibles à tout un chacun.

Dans les lieux qui sont accessibles au public, recueillir le consentement préalable exprès de tous les individus s'avère d'emblée impossible. Pénétrer dans une zone filmée aux abords de laquelle sont placardés des avertissements *ad hoc* pourrait tout au plus exprimer un consentement implicite au traitement de ses données sensibles. Si, sur le domaine privé, il est admissible de présumer qu'un tel consentement puisse être donné librement, puisqu'il est toujours possible de garer sa voiture dans un autre parking ou de faire ses courses dans un autre magasin, il faut admettre que le consentement sur le domaine public risque d'être de plus en plus forcé, au fur et à mesure que la vidéosurveillance s'étend dans l'espace public. Contrairement à ce qui vaut pour le domaine privé accessible au public, régi par le droit privé, le consentement à la vidéosurveillance du domaine public n'est pas formellement exigé, pour autant que les exigences constitutionnelles de la légalité et de la conformité aux libertés soient respectées. Or, un consentement forcé, de fait, ne peut justifier une exception à la base légale formelle telle que posée à l'article 17 al. 2 let. c LPD. Selon la doctrine, le consentement doit en effet être exprès, volontaire et éclairé [18].

S'agissant de rendre ces données "*accessibles à tout un chacun*" (art. 17 al. 2 let. c LPD), il faut admettre que, s'il est vrai que porter en public des symboles religieux ostensibles équivaut à informer tout le monde d'une donnée personnelle sensible et que la couleur de peau révèle, *nolens volens*, "*l'appartenance à une race*" (art. 3 let. c ch. 2 LPD), l'accomplissement de certaines pratiques trahissant un état de santé déficient, révélant une appartenance religieuse ou exprimant une orientation sexuelle, jouissent de la protection de la sphère privée, même s'ils sont accomplis en public. De tels cas ne sont pas rares, au point qu'ils ne se trouveraient quasiment jamais enregistrés par des dispositifs de vidéosurveillance. Nous pouvons en déduire que cette troisième exception ne saurait s'appliquer telle quelle à la vidéosurveillance des lieux publics, dans la mesure où un certain nombre de données sensibles ne sont, par ce biais, pas rendues accessibles "*à tout un chacun*", et encore moins à l'autorité qui recourt à la vidéosurveillance, mais aux passants seulement.

La loi fédérale sur la protection des données, dans sa révision du 24 mars 2006 [19], précise l'article 17 al. 2 let. c LPD, en proposant de donner "*plus de poids au droit, pour la personne concernée, de s'opposer au traitement, même si elle a rendu ses données accessibles à tout un chacun*." La personne pourrait ainsi s'opposer au traitement "*quand bien même elle aurait rendu ses données accessibles à tout un chacun*" [20].

Dans tous les cas de figure, lorsque les techniques de vidéosurveillance de dernière génération traitent des profils de la personnalité, l'exception de l'accessibilité générale ne trouve pas à s'appliquer, car la diffusion porte sur les données sensibles et non sur l'assemblage de données que constitue le profil de personnalité.

3.1.2. La vidéosurveillance visant au maintien de la sécurité de l'Etat

Le Conseil fédéral a adopté le 27 juin 2001 l'ordonnance sur la sécurité relevant de la compétence fédérale (OSF) [21]

---

réglementant la vidéosurveillance "*afin de déceler les dangers qui menacent des personnes et leurs biens, des bâtiments de la Confédération ainsi que des représentations étrangères et des organisations internationales, pour autant que celles-ci consentent à l'enregistrement de ces données*" (art. 15 al. 1er OSF) et exigeant notamment la destruction des enregistrements au plus tard après 24 heures (art. 15 al. 3 OSF).

Contrairement à l'article 14 al. 2 let. f de la loi fédérale instituant des mesures visant au maintien de la sûreté intérieure (LMSI) [22], qui concerne la vidéosurveillance invasive [23], les articles 22 et suivants ne prévoient pas expressément le recours à la vidéosurveillance.

Il importe donc d'examiner tout d'abord si les exceptions de l'article 17 al. 2 LPD s'appliquent. Tel n'est pas le cas. La réserve du consentement en faveur des représentations étrangères et des organisations internationales posée à l'article 15 al. 1er OSF ne doit pas induire en erreur, car l'art. 17 al. 2 let. c LPD exige le consentement de la personne concernée (au sens de l'art. 3 let. b LPD), c'est-à-dire les personnes entrant dans le champ de vision des caméras et enregistrées par le système technique. Il est donc douteux que l'art. 15 OSF soit conforme à l'art. 17 al. 2 LPD.

En outre, en fonction du système utilisé, la gravité de l'atteinte exigerait l'adoption d'une base légale formelle plus précise sur le fondement des articles 36 al. 1er et 164 al. 1er let. b Cst. Telle serait le cas si la vidéosurveillance mise en œuvre devait être informatisée.

3.1.3. La vidéosurveillance de la frontière

Le Conseil fédéral a adopté le 26 octobre 1994 l'ordonnance réglant la surveillance de la frontière verte au moyen d'appareils vidéo [24], dont le but est de "*garantir la sécurité de la ligne des douanes et la perception des droits ainsi que de surveiller le franchissement de la frontière*" (art. 1er). Elle exige notamment l'effacement des enregistrements dans un délai de trois semaines au plus tard (art. 3 al. 2) [25].

On peut transposer *mutatis mutandis* à cette ordonnance le raisonnement relatif à l'ordonnance sur la sécurité, car l'article 27 al. 1er de la loi fédérale sur les douanes [26], qui lui sert de fondement, ne prévoit pas expressément le recours à la vidéosurveillance. L'ordonnance n'est ainsi pas compatible avec l'article 17 al. 2 LPD [27].

3.1.4. La vidéosurveillance dans les transports publics

Le 5 décembre 2003, le Conseil fédéral a adopté l'ordonnance sur la vidéosurveillance des Chemins de fer fédéraux [28], qui s'applique aux trains et aux installations ferroviaires afin de protéger les passagers, l'exploitation et les infrastructures (art. 2 al. 1er) contre les agressions et les incivilités (art. 2 al. 2 let. a) notamment. Les enregistrements doivent être analysés au plus tard le jour ouvrable qui suit l'enregistrement, puis détruits en principe dans les 24 heures (art. 4 al. 1er et 2). L'ordonnance précise également que le domaine secret des personnes ne peut être surveillé (art. 179quater CP). Bien qu'elle relève de l'évidence, cette précision symbolique montre la difficulté qu'il y a, dans des lieux aussi confinés que les transports publics, à ne pas empiéter sur la sphère privée ou le domaine secret des individus.

Cette ordonnance a été critiquée, à juste titre, au motif qu'elle décrit le but de la surveillance de manière très générale et sans concrétisation du principe de proportionnalité [29]. En outre, on lui reprochera l'imprécision du but de la lutte contre les "*incivilités*" prévue à l'article 2 al. 2 let. a. Ce terme est beaucoup trop vague, trop subjectif, et surtout juridiquement indéfini, pour être opérationnel. Mieux vaut se tenir au critère de l'infraction pénale, comme le fait à juste titre le législateur bâlois.

La Confédération a reconnu dans ce cas la faiblesse de la base légale [30] et a proposé d'adopter un nouvel article 16b, intitulé "vidéosurveillance", malheureusement rédigé de manière trop vague, dans le cadre du projet de modification de la loi sur les chemins de fer (LCdF) [31]. Cette disposition se rapporte à la surveillance de l'infrastructure seulement, définie à l'article 62 al. 3 LCdF, alors que l'ordonnance en vigueur vise en outre la protection des passagers et de l'exploitation [32].

Les commissaires suisses à la protection des données ont recommandé en 2004 aux cantons qui n'avaient pas encore entamé des travaux législatifs en vue de la création d'une base légale pour la surveillance par vidéo dans les transports publics de ne pas se lancer dans une procédure législative en raison de la révision de la législation fédérale sur ce point [33].

3.1.5. La vidéosurveillance dans les maisons de jeu

L'ordonnance du Conseil fédéral sur les maisons de jeu (OLMJ), du 24 septembre 2004 [34], prévoit un certain nombre de règles, obligeant les maisons de jeu à s'équiper d'un système de vidéosurveillance (art. 30 al. 1er). Cette réglementation est singulière en ce qu'elle contraint les casinos à installer de tels systèmes. Contrairement à la pratique, répandue, fixant une limite *maximale* de conservation des données, l' OLMJ fixe une durée *minimale* de quatre semaines durant lesquelles les enregistrements doivent être conservés en lieu sûr (art. 30 al. 3) et en interdit expressément l'effacement ou la destruction avant la décision de la commission fédérale des maisons de jeu en cas de dérèglement du système de vidéosurveillance ou lorsque des infractions ou des irrégularités de jeu ont été observées et filmées (art. 30 al. 6). L'ordonnance prévoit également une sous-délégation au département afin d'édicter des dispositions supplémentaires sur les exigences auxquelles le système de vidéosurveillance doit satisfaire et sur son exploitation [35].

De telles règles sont particulièrement intrusives, compte tenu notamment de la précision des enregistrements, de la permanence et de l'individualisation du contrôle. Elles ne reposent pourtant que sur une délégation législative autorisant le Conseil fédéral à définir "*les exigences auxquelles le programme de mesures de sécurité*" doit satisfaire (art. 14 al. 3 LMJ [36)]. Il n'est pas certain que cette clause puisse valablement servir de base légale au système de vidéosurveillance institué.

3.2. Les règles cantonales

A ce jour, Bâle-Ville est le seul canton qui dispose d'une base légale spécifique régissant de manière générale la vidéosurveillance dissuasive des lieux ouverts au public [37]. Quelques cantons ont édicté dans ce domaine des actes non obligatoires [38]. Tel est le cas de Zurich [39], Bâle-Campagne [40], Lucerne [41] et Fribourg [42]. Plus spécifiquement, certains cantons disposent de bases légales autorisant la vidéosurveillance invasive dans ces cas particuliers, tels que les manifestations, ou l'usage dans un cadre policier.

A défaut d'une base légale spécifique, les cantons peuvent-ils se fonder sur leur réglementation générale en matière de protection des données pour autoriser la vidéosurveillance par des organes publics cantonaux et communaux? La réponse dépend des exigences posées pour le traitement des données sensibles ainsi que du degré d'atteinte aux libertés, dépendant lui-même de l'agencement du dispositif.

3.2.1. Bâle-Ville

Bâle-Ville est, pour l'instant, le seul canton à disposer d'une base légale formelle spécifique relative à la vidéosurveillance dissuasive des lieux publics et accessibles à tous. L'article 6a de la loi cantonale sur la protection des données [43], en vigueur depuis le 1er février 2005 [44], instaure une procédure d'autorisation (al. 1er), limite la finalité du dispositif à la protection des personnes et des biens contre des actes pénalement répréhensibles dans les seuls lieux nécessaires pour atteindre ce but (al. 2), requiert de communiquer l'organe responsable et de rendre les modalités de la vidéosurveillance reconnaissables (al. 3) et exige d'exploiter les données personnelles recueillies au plus tard le jour ouvrable suivant et de les détruire à la suite dans les 24 heures, sous réserve d'une utilisation dans le cadre d'une procédure pénale ou civile (al. 4).

Sur ce fondement, le Conseil d'Etat a adopté le 4 janvier 2005 une ordonnance sur la vidéosurveillance, qui est entrée en vigueur le 1er février 2005 [45]. Elle précise la notion de "lieu public" en la limitant aux lieux dont les organes publics cantonaux disposent (art. 1er al. 3). Cette restriction découle logiquement de la conception législative retenue en droit suisse pour réglementer la vidéosurveillance.

L'ordonnance bâloise étend cependant le champ d'application de la loi aux lieux publics non accessibles à tous (art. 1er al. 2). S'agit-il du patrimoine administratif? En partie seulement, car le patrimoine administratif comporte également des parties accessibles au public. Le législateur eût bien été inspiré de le préciser, afin d'éviter tout problème de délégation législative.

Le principe de finalité est rappelé à l'article 3, exigeant que les caméras soient disposées de façon à ne viser que les lieux à surveiller et qu'elles ne doivent être exploitées que durant les moments nécessaires, ainsi qu'à l'article 5 al. 3 précisant que les enregistrements ne peuvent être utilisés que dans le cadre des buts visés.

3.2.2. Genève

La législation genevoise sur la protection des données est aujourd'hui surannée. Le canton de Genève a pourtant joué un rôle pionnier en ce domaine, en adoptant en 1976 [46], puis en 1981, la loi sur les informations traitées automatiquement par ordinateur (LITAO) [47] et son règlement d'exécution [48]. Cette législation, qui s'applique aux seuls "*fichiers de l'Etat, des communes et des établissements de droit public, relatifs aux personnes et préparés aux fins de traitement automatique, ainsi qu'à toutes les données qui sont stockées et à tous les résultats du traitement de ces fichiers*" (art. 1er LITAO), ne vise que les fichiers informatiques, rendant la protection des données ainsi lacunaire. L'accès aux fichiers de police, médicaux ou judiciaires est réglé dans des lois spéciales (art. 9 LITAO).

Le développement des technologies de l'information a rendu cette loi obsolète [49] et, partant, difficilement applicable. Elle est source de lourdeurs, dans la mesure où elle n'est pas appliquée de façon systématique et régulière [50].

Nonobstant, dans la mesure où les dispositifs de vidéosurveillance ne sont désormais plus analogiques mais numériques, ils entrent dans le champ d'application de cette loi dès lors qu'ils sont mis en œuvre par l'Etat, les communes ou les établissements de droit public (art. 1er LITAO). Bien que cette loi ainsi que son règlement d'exécution soient trop vagues et trop indéterminés pour satisfaire aux exigences de précision de

la base légale dans tous les cas où les dispositifs de vidéosurveillance portent atteinte aux libertés, le Conseil d'Etat s'est fondé sur l'article 2 al. 1er LITAO pour autoriser, sur préavis de la commission de contrôle de l'informatique de l'Etat, la création et l'exploitation par les Transports publics genevois d'un système de surveillance par caméras vidéos à l'intérieur des véhicules [51], afin de garantir la sécurité, de prévenir des agressions ou des déprédations et de fournir les moyens de preuve en cas de procédure administrative ou judiciaire. Le délai pour effacer les bandes enregistrées, initialement fixé à 24 heures, a été porté à sept jours en principe après l'enregistrement [52]. En l'état, les bases légales font donc défaut dans le canton de Genève pour autoriser la vidéosurveillance par les organes publics cantonaux. Un projet cantonal sur la protection des données a été accepté par le Conseil d'Etat (voir ci-dessous note 37).

3.3. Des règles communales?

Les communes sont-elles autorisées à réglementer la vidéosurveillance sur leur territoire? La réponse dépend du droit cantonal. On se limitera à étudier la question dans deux cantons dont, pour l'instant, l'un limite les compétences communales au contraire de l'autre [53].

3.3.1. Les communes bernoises

En droit bernois, la doctrine récente est d'avis qu'en matière de vidéosurveillance dissuasive des lieux publics, les communes ne sont pas compétentes pour légiférer. Une base légale cantonale spécifique doit donc être créée. Selon l'article 9 al. 1er de la loi sur la police du 8 juin 1997, la police communale "*accomplit sur le territoire communal les tâches de la police de sûreté et de la police routière*". Il incombe à la police de sûreté "*d'empêcher la commission imminente d'actes punissables ou d'interrompre la commission de tels actes*". La prévention de dangers abstraits, tels que la vidéosurveillance dissuasive les vise, est dès lors exclue. Même si l'on devait admettre qu'une surveillance limitée à des endroits névralgiques, théâtres répétés d'infractions pénales, répond à l'exigence de la commission imminente d'actes punissables, le catalogue des mesures de police défini par la loi, qui ne prévoit pas la vidéosurveillance, s'opposerait à une extension de la compétence municipale en raison du caractère exhaustif du catalogue.

La seule compétence de vidéosurveillance reconnue aux communes concerne la surveillance du trafic, dans la mesure où cette tâche ne requiert pas d'individualiser les véhicules ni d'identifier les chauffeurs et rentre dans le cadre de l'article 9 al. 1er de la loi, disposant que la police communale accomplit sur le territoire communal les tâches de la police routière.

Les communes n'ont, enfin, aucune compétence réglementaire en matière de vidéosurveillance invasive (police judiciaire) [54].

3.3.2. Les communes genevoises

La question de savoir si les communes genevoises sont habilitées à légiférer en matière de vidéosurveillance pour créer ainsi la base légale, qui fait défaut en droit fédéral et en droit cantonal, mais sans laquelle les restrictions à la vie privée qu'implique cette surveillance ne sont pas conformes à la constitution se pose sous deux angles différents, qui sont complémentaires: compétence du conseil municipal de délibérer en la matière et pouvoir des agents de sécurité municipaux d'exploiter ce type de surveillance.

La loi sur l'administration des communes, du 13 avril 1984 (LAC) [55], prévoit que le conseil municipal exerce des fonctions délibératives et consultatives (art. 29 al. 1), seules les premières étant en principe soumises au référendum (art. 29 al. 2). Elle énumère ensuite limitativement toutes les matières sur lesquelles le conseil municipal peut délibérer (art. 30 al. 1er). Or, cette longue liste ne se réfère ni à la vidéosurveillance, ni au domaine public. En revanche, aux termes de l'art 30 al. 2 LAC, "*le conseil municipal peut également adopter, sous forme de délibération, des règlements ou des arrêtés de portée générale régissant les domaines relevant de la compétence des communes*".

Le patrimoine administratif compte sans doute parmi les domaines qui relèvent de la compétence des communes, au sens de cette disposition. Il en va de même du domaine public municipal: s'il est vrai qu'en matière de réglementation du domaine public, en particulier des différents usages que les particuliers peuvent en faire, le droit genevois est largement centralisé [56], il n'en reste pas moins que l'aménagement

pratique et concret des biens rentrant dans leur domaine public relève de la compétence des communes [57]. C'est si vrai que l'on imagine mal le canton prendre des dispositions concrètes concernant l'aménagement d'un parc municipal ou d'une place de village, qui relèvent à n'en pas douter de l'autonomie communale, même dans un canton comme Genève où cette autonomie est traditionnellement fort réduite [58].

Une commune genevoise peut donc en principe se fonder sur la clause générale de l'article 30 al. 2 LAC pour édicter un règlement en matière de vidéosurveillance sur son domaine public. C'est ce qu'a fait la commune du Grand-Saconnex qui a obtenu l'autorisation fondée sur la LITAO en mars 2006 [59].

4. La conformité aux libertés

4.1. Les libertés en jeu

Plusieurs libertés sont potentiellement en jeu: la liberté personnelle, et plus particulièrement la triple garantie de l'intégrité physique et psychique et de la liberté de mouvement (art. 10 al. 2 Cst.), le droit au respect de la sphère privée (art. 13 al. 1 Cst. et 8 CEDH), le droit d'être protégé contre l'emploi abusif des données personnelles (art. 13 al. 2 Cst.) et la liberté de réunion (art. 22 Cst.).

4.1.1. La liberté personnelle

Le droit à *l'intégrité physique* protège les individus contre toute intervention étatique sur leur corps, même celles qui passent inaperçues et ne laissent pas de trace [60]. Le Tribunal fédéral a jugé en 1981 que le fait de photographier le visage d'un suspect et de prendre ses empreintes digitales portait atteinte à sa liberté personnelle et au droit de la personnalité protégé par la constitution [61]. Deux ans plus tard, il a ajouté que ces actes touchaient "*sans conteste la sphère intime de l'individu et (constituaient), partant, une atteinte à la liberté personnelle*" [62]. Mais il s'agit d'arrêts relativement anciens qu'il est permis d'interpréter, en ce sens que l'atteinte à l'intégrité corporelle résidait davantage dans l'empreinte digitale que dans la prise de photo.

Quant à *l'intégrité psychique*, elle englobe selon la jurisprudence toutes les libertés élémentaires dont l'exercice est indispensable à l'épanouissement de la personne humaine [63], ou encore toutes les manifestations élémentaires de la personnalité humaine. Le Tribunal fédéral a jugé en 1981 que la protection de la sphère privée faisait partie de ces libertés élémentaires [64], mais cette qualification a perdu sa raison d'être depuis que la Constitution fédérale garantit expressément

---

le droit au respect de cette sphère. En revanche, selon la doctrine, l'article 10 al. 2 Cst. protège de façon générale "l'autodétermination individuelle" (*Schutz der individuellen Selbstbestimmung*), qui comprend notamment le droit de participer à la vie sociale, mais aussi celui d'être laissé seul, à l'abri du regard des autres [65]. Pour le Tribunal fédéral, la liberté personnelle constitue toujours "*une garantie fondamentale à la protection de la personnalité*" [66].

La *liberté de mouvement*, assurant traditionnellement à l'individu une protection contre les arrestations et les détentions arbitraires [67] , protège la liberté d'aller et de venir. Cette liberté peut être touchée par d'autres mesures non privatives de liberté au sens strict [68] , à l'instar des restrictions de circulation ou de l'obligation d'avoir constamment sur soi des papiers d'identité [69]. La vidéosurveillance n'empêche pas physiquement une personne de se déplacer dans un lieu filmé. Elle constitue en revanche une barrière psychologique incontestable pour les personnes qui, pour divers motifs, ne veulent pas être filmées. De surcroît, le but déclaré de la vidéosurveillance consiste précisément à filtrer le passage de certains endroits en barrant l'accès aux personnes dont le comportement est en contradiction avec les buts d'intérêt public que la vidéosurveillance a pour mission de remplir. Le Conseil fédéral [70], et à sa suite le Tribunal fédéral [71], considèrent que la liberté de mouvement peut être atteinte par des systèmes de surveillance ou de contrôle destinés à surveiller le comportement des travailleurs à leur poste de travail. La vidéosurveillance constitue donc un risque pour la liberté d'aller et venir [72].

Couplée au droit au respect de la sphère privée, et replacée dans le contexte d'une traçabilité toujours croissante des déplacements des individus, la liberté de mouvement devrait évoluer et garantir dorénavant la liberté d'aller et venir *anonymement* [73] . L'extension du réseau de caméras sur le domaine public, le développement de mécanismes de reconnaissance et de suivi visuels de personnes au sein de foules, ainsi que les progrès des systèmes de géolocalisation, permettent en effet à un opérateur de suivre à la trace une

personne déterminée en permanence et en temps réel [74], l'empêchant ainsi d'aller et de venir de manière anonyme.

4.1.2. Le droit au respect de la sphère privée

Garanti par les articles 13 al. 1er Cst., 8 CEDH et 19 Pacte II, le droit au respect de la sphère privée protège de façon générale l'identité, la réputation, les relations sociales et les comportements intimes de chaque personne physique, bref: toutes les informations relatives à une personne qui ne sont pas accessibles au public [75], "*eine Summe privater Lebenssachverhalte, die man von der Öffentlichkeit abgeschirmt haben will*" [76] . Ainsi, le champ de protection de l'article 13 Cst. est limité négativement par le critère de l'accessibilité au public (*Öffentlichkeit*): un comportement donné ne tombe pas dans ce champ de protection lorsqu'il est publiquement reconnaissable, visible et qu'il n'existe pas d'intérêt à ce qu'il soit gardé secret ou confidentiel. En revanche, lorsqu'un tel intérêt existe, un comportement donné est protégé par la garantie constitutionnelle de la vie privée, même s'il est observé sur le domaine public [77] . Ainsi, selon la doctrine récente, "*la personne qui n'exerce pas de fonction publique ne doit pas accepter qu'une autorité étatique enregistre en public ses paroles ou son image*" [78]. Pour la Cour européenne des droits de l'homme, la garantie de la vie privée doit permettre d'assurer "*le développement, sans ingérences extérieures, de la personnalité de chaque individu dans les relations avec les semblables*" [79].

La Cour européenne des droits de l'homme a jugé, le 17 juillet 2003, que "*la surveillance des faits et gestes d'une personne dans un lieu public au moyen d'un dispositif photographique ne mémorisant pas les données visuelles ne constitue pas en elle-même une forme d'ingérence dans la*

**** AJP/PJA 2006 page 933 ****

vie privée" [80] et que " *l'utilisation ordinaire de caméras de surveillance dans des rues et dans des édifices publics, tels que des centres commerciaux ou des commissariats, où elles visent un but légitime et identifiable, ne soulève en elle-même aucune difficulté au regard de l'article 8 § 1 de la Convention*." [81] La vidéosurveillance utilisée à des fins de sécurité dans un lieu public ou accessible au public ne porte pas atteinte à la sphère privée dès lors que les données ainsi obtenues ne sont pas enregistrées. La Cour l'a précisé dans l'affaire précitée: "*En revanche, le fait de recueillir systématiquement de telles données* (vidéosurveillance dans un lieu public) *et de les mémoriser peut soulever des questions liées à la vie privée*" [82].

Cette conclusion ne saurait cependant valoir qu'en l'état actuel de la technique. Lorsque la vidéosurveillance s'informatise, elle recèle un potentiel d'atteinte à la sphère privée indépendamment de l'enregistrement des données.

En 2003, le Tribunal fédéral des assurances a relevé, dans un bref passage, que la vidéosurveillance effectuée par un détective privé, mais utilisée par l'autorité pour refuser à la personne surveillée des prestations d'assurance accidents, constituait une atteinte au respect de la vie privée garanti l'article 13 Cst. [83] Toujours dans un cas de vidéosurveillance invasive, le Tribunal fédéral a jugé, en 2005, dans un considérant non publié, que la vidéosurveillance par la police d'un garage souterrain, espace "quasi public" dans lequel la personne surveillée ne demeure qu'un temps limité, et dont le dispositif efface automatiquement les enregistrements après 24 heures, ne constituait pas une atteinte grave aux droits de la personnalité du recourant [84].

Dans toutes les hypothèses, la gravité doit s'apprécier en fonction de l'ensemble des circonstances concrètes du cas. Il faut ainsi tenir compte par exemple de la permanence et de l'individualisation de la surveillance. Le Tribunal fédéral a précisé qu'un système de localisation par satellite d'une flotte de voiture qui permettrait à l'employeur de suivre de manière continue et en temps réel le trajet emprunté par les véhicules utilisés par les employés serait disproportionné [85]. Il a souligné que "*tandis qu'une caméra braquée en permanence sur un employé au guichet d'une banque est, abstraitement, de nature à provoquer une atteinte importante à la personnalité du travailleur concerné, il n'en est rien si cette même caméra n'est pas reliée à une salle de contrôle, mais qu'elle ne fait qu'enregistrer sur une bande, pour des motifs de sécurité, ce qui se passe, et que l'enregistrement est ensuite détruit, sans être utilisé, sous réserve d'exceptions bien définies à l'avance (par exemple au cas où un délit est commis)*." [86] Dès lors, la vidéosurveillance en temps réel porterait une atteinte grave (sans précision sur l'enregistrement éventuel des données) lorsque la caméra est braquée en permanence sur une personne déterminée alors que, dans ces mêmes circonstances, l'enregistrement avec visionnement ultérieur subsidiaire ne porterait pas une

atteinte importante. Il nous paraît toutefois excessif de prétendre, au vu de la jurisprudence de la Cour européenne des droits de l'homme exposée précédemment, que l'atteinte ne serait pas importante dans le cas de l'enregistrement.

4.1.3. Le droit d'être protégé contre l'emploi abusif de données personnelles

En consacrant à l'article 13 al. 2 Cst. le droit de toute personne "*d'être protégée contre l'emploi abusif des données qui la concernent*", le constituant de 1999 a fait sienne la jurisprudence du Tribunal fédéral, qui avait déduit la protection des données personnelles et le droit de consulter ces données de l'article 4 de la Constitution fédérale du 29 mai 1874 (aCst.) et de la garantie, à l'époque non écrite, de la liberté personnelle [87]. La doctrine contemporaine parle à ce propos du droit à l'autodétermination informationnelle" (*informationnelles Selbstbestimmungsrecht*) [88], qui va plus loin que le simple emploi abusif de données: chaque personne doit pouvoir déterminer elle-même si et dans quel

---

but les informations récoltées par l'Etat ou par des particuliers sur elles peuvent être traitées. C'est seulement lorsque chaque personne se voit reconnaître le droit à cette autodétermination informationnelle qu'elle peut s'opposer à ce que l'Etat ou des tiers l'observent, la surveillent en permanence, la contrôlent, la mettent à nu ou la disqualifient de quelque manière que ce soit [89].

Ainsi, la saisie, la conservation et l'utilisation de données personnelles constituent des atteintes au droit garanti par l'article 13 al. 2 Cst. Par données personnelles, il faut entendre selon l'article 3 let. a LPD toutes les informations qui se rapportent à une personne identifiée ou identifiable, c'est-à-dire toutes les informations sur les caractéristiques physiques, psychiques, sociales ou politiques d'un individu, comme notamment les empreintes digitales, les analyses ADN, les photos ou les fiches. La protection constitutionnelle des données personnelles s'étend ainsi à toute récolte et à tout traitement de celles-ci, indépendamment de la méthode appliquée. Elle englobe le droit d'être informé de l'existence de telles données, donc un droit à la consultation des fichiers et des dossiers, ainsi que le droit d'obtenir la rectification des données inexactes et l'élimination des données inutiles [90].

Les données obtenues par vidéosurveillance, qu'elles soient sous forme de séquences d'images ou de sons, qu'elles soient enregistrées ou non, sont susceptibles de contenir des données personnelles chaque fois que les images filmées se rapportent à une ou plusieurs personnes identifiées ou identifiables [91]. *A contrario*, elles n'en constituent pas si les personnes ne sont pas identifiables, par exemple lorsque la résolution des images est trop faible, ou lorsqu'aucune personne ne pénètre dans le champ des caméras [92].

De manière générale, les données personnelles transitant dans les dispositifs de vidéosurveillance ne sont pas des données ordinaires mais des *données sensibles* au sens de l'article 3 let. c LPD, dans la mesure où elles sont de nature à informer sur la santé, la sphère intime ou l'appartenance à une race (art. 3 let. c ch. 2 LPD) ou sur les opinions ou les activités religieuses (art. 3 let. c ch. 1er LPD). La couleur de la peau, l'état de santé général, le port de symboles religieux, l'accomplissement de certaines pratiques révélant une appartenance religieuse ou trahissant une orientation sexuelle sont des éléments que les techniques de vidéosurveillance peuvent mettre en évidence [93].

4.1.4. La liberté de réunion

La liberté de réunion garantie à l'article 22 Cst. est également visée. La barrière psychologique que constitue la vidéosurveillance, comme nous l'avons montré ci-dessus pour la liberté de mouvement, peut empêcher de la même manière certains individus de se réunir librement [94]. La question se pose pratiquement lorsque la police filme les participants à une manifestation. Cette mesure pourrait selon les circonstances dissuader d'organiser une manifestation (atteinte au droit de convoquer une réunion), empêcher certaines personnes de s'y rendre (atteinte au droit de participer à une manifestation) ou conduire à assimiler un passant à la manifestation contre son gré (droit de se tenir à l'écart d'une réunion).

4.2. Une atteinte aux libertés

En conclusion, la vidéosurveillance non informatisée permettant d'identifier des personnes sans enregistrement ne porte en principe atteinte ni à la liberté personnelle, ni à la sphère privée, ni à la maîtrise informationnelle, ni à la liberté de réunion. Seules des circonstances particulières peuvent conduire à établir

---

une atteinte, à l'instar de la permanence et l'individualisation de la surveillance [95].

En revanche, la vidéosurveillance avec enregistrement simple, effacé automatiquement après une brève durée, constitue selon nous une atteinte légère. Elle est plus intrusive si elle est doublée d'un suivi en temps réel en salle de contrôle. Il en va de même si l'enregistrement est en haute résolution, doté de caméras orientables et zoomables à distance.

L'atteinte est grave si la vidéosurveillance est doublée d'un traitement informatisé, permettant en particulier d'établir des profils de personnalité éventuellement en couplage avec des bases de données biométriques, de suivre automatiquement une scène, d'initier des alarmes en fonction de l'analyse de comportements types ou de caractéristiques prédéfinies. Le recours à Internet pour le transit des données, leur visualisation ou le pilotage des caméras augmente l'atteinte potentielle, en particulier en l'absence d'un système de cryptage permettant aisément de diffuser ces données sans restriction.

Le critère de l'enregistrement n'est donc pas absolu pour distinguer l'existence ou non d'une atteinte et qualifier sa gravité. Il s'agit d'un élément, certes important, à prendre en considération dans le contexte plus général des possibilités techniques constamment en évolution. Il en découle que l'absence d'enregistrement peut selon les circonstances conduire à une atteinte, même grave. Dans tous les cas, en revanche, l'existence d'un enregistrement, même simple, est constitutif d'une atteinte aux libertés.

4.3. Les finalités d'intérêt public

Pour être conforme à la constitution, une restriction aux libertés prévue par la loi doit être justifiée par un intérêt public ou par la protection d'une liberté d'autrui (art. 36 al. 2 Cst.). L'article 8 CEDH, qui garantit le respect de la sphère privée (al. 1er), admet que l'Etat peut restreindre cette garantie pour protéger la sécurité nationale, la sûreté publique, le bien-être économique du pays, la défense de l'ordre et la prévention des infractions pénales, la protection de la santé ou de la morale, ou la protection des droits et libertés d'autrui (al. 2).

La vidéosurveillance par les autorités du domaine public et du patrimoine administratif accessible au public vise deux buts principaux: prévenir des actes de vandalisme et identifier les auteurs de tels actes pour les poursuivre. La prévention et la répression d'infractions pénales comptent parmi les motifs qui peuvent justifier des restrictions aux libertés. Le Tribunal fédéral a jugé que "*la prévention d'actes délictuels futurs et la poursuite d'actes délictuels commis sont toujours dans l'intérêt public* " [96]. D'une manière plus générale, ces deux buts visent à augmenter la sécurité de la population ou, pour le moins, à diminuer le sentiment d'insécurité [97]. Si, en rapport avec ce dernier objectif de nature plus psychologique, il est indéniable qu'il existe un intérêt public à ce que la population se sente davantage sécurisée par la présence de caméras vidéos à certains endroits stratégiques, une controverse existe sur le type de vidéosurveillance à mettre en œuvre pour atteindre ce but [98]. Implicitement, ce type de technologie vise à accroître l'efficacité des tâches de surveillance, pour autant que l'on démontre que cela permette "*de rationaliser la surveillance et d'économiser du personnel de surveillance*", tout en pouvant constituer "*un excellent moyen de conserver des preuves du passage d'une personne à un endroit donné*" [99]. Nous reviendrons sur ces buts lors de l'examen de la proportionnalité.

Dans tous les cas de figure, le but doit être défini précisément. Il n'est ainsi pas admissible de mentionner la lutte contre les "*incivilités*" comme le fait pourtant l'ordonnance sur la vidéosurveillance CFF du 5 décembre 2003 (art. 2 al. 2 let. a).

Du point de vue du droit de la protection des données personnelles, la détermination de la finalité poursuivie est essentielle pour juger de l'admissibilité du traitement. Le principe de finalité exige que *"les données personnelles ne doivent être traitées que dans le but qui est indiqué lors de leur collecte, qui est prévu par une loi ou qui ressort des circonstances*." (art. 4 al. 2 LPD). La préposée fribourgeoise à la protection des données donne comme exemple dans son aide-mémoire concernant la surveillance vidéo effectuée par des organes publics cantonaux et communaux dans des lieux et bâtiments publics [100] celui d'une caméra installée dans un garage souterrain pour empêcher des atteintes aux personnes qui capterait des élèves fumant un joint. L'utilisation de telles images à l'encontre de ces derniers serait contraire au principe de finalité.

4.4. Le respect du principe de la proportionnalité

Les restrictions aux libertés doivent, pour être conformes à la constitution, respecter le principe de la proportionnalité (art. 36 al. 3 Cst.). Celui-ci exige de façon générale un rapport raisonnable entre le but d'intérêt public visé, le moyen choisi pour l'atteindre et le respect de la liberté impliquée [101].

4.4.1. La règle de l'aptitude

La première question à examiner en rapport avec le principe constitutionnel de la proportionnalité est celle de savoir si la vidéosurveillance est apte à atteindre les buts d'ordre public visés, en l'espèce la prévention ou la poursuite d'infractions contre des personnes ou des biens.

La réponse est délicate. On peut certes admettre que la présence de caméras vidéos à un endroit déterminé peut inciter les personnes qui s'y trouvent à ne pas commettre des infractions, de peur d'être repérées et, le cas échéant, poursuivies. Encore faut-il distinguer entre une vidéosurveillance en temps réel avec un suivi constant par un personnel qualifié, éventuellement par des méthodes informatisées, et une vidéosurveillance se limitant à un simple enregistrement des données, visionnées *a posteriori* uniquement en cas de problème. Le second procédé n'est véritablement utile qu'à la recherche des auteurs d'infractions, une fois celles-ci commises.

**** AJP/PJA 2006 page 936 ****

Les études scientifiques récentes montrent qu'il existe un doute sur l'efficacité réelle de la vidéosurveillance. La direction de la recherche, du développement et des statistiques du Département de l'intérieur anglais a publié en février 2005 l'évaluation la plus complète à ce jour de l'efficacité de la vidéosurveillance [102]. Cette évaluation conclut dans un premier temps, à la lecture des études publiées jusqu'alors, que les recherches sur l'efficacité conduisent à des conclusions divergentes. Alors que de nombreuses recherches mettent des succès en évidence, de nombreuses autres relatent des échecs. Les expériences concluantes, notamment la protection des parkings, sont difficiles à interpréter, en ce sens que la vidéosurveillance a été introduite à côté d'autres mesures, ne permettant pas de distinguer la part propre de la vidéosurveillance dans les succès. Parfois même l'installation de caméras a pour effet d'augmenter, de façon non significative il est vrai, le taux de criminalité observée dans la zone considérée, en raison probablement d'une augmentation du taux de communication des infractions. L'efficacité dépend du type d'infraction: plus grande pour les infractions préméditées ou planifiées (par exemple le vol de voiture), elle est plus faible pour les actes répréhensibles spontanés (par exemple les violences commises contre les personnes sous l'empire de l'alcool). Elle dépend également de facteurs fort divers, à l'instar des performances des caméras et de la qualité de l'enregistrement, des conditions de luminosité, de la présence active des agents dans les salles de surveillance, de leurs compétences et des relations avec les forces de l'ordre lorsqu'il s'agit d'intervenir, de la combinaison avec d'autres mesures de réduction de la criminalité, ainsi que du type de lieu: les lieux fermés, avec un nombre limité d'accès, comme les parkings, se prêtent mieux à ce type de surveillance que les endroits ouverts. La densité de la couverture est également un facteur déterminant. Enfin, il reste à interpréter les chiffres dans leur contexte plus général: la différence éventuellement observée de l'évolution du taux de criminalité au lieu de la surveillance doit être mise en relation avec l'évolution générale de ce même taux dans la société durant la période considérée.

S'il est communément admis que la vidéosurveillance déplace géographiquement la scène criminologique, l'évaluation anglaise ne trouve cependant que peu de preuves pour étayer cette hypothèse [103]. Tout dépend en réalité des objectifs assignés à la vidéosurveillance: si celle-ci est censée inciter les citoyens à trier leurs ordures dans l'enceinte d'une déchetterie, elle sera probablement plutôt efficace. Le raisonnement ne peut cependant pas être étendu si l'objectif s'inscrit dans le cadre plus vaste de la lutte contre la prolifération des décharges sauvages. En ce cas, le risque est grand que le premier objectif conduise à un déplacement de la problématique, ne résolvant en rien le problème général.

L'évaluation tend à montrer que ni le but de diminuer la criminalité n'a pu être atteint par les dispositifs de vidéosurveillance, ni celui d'augmenter le sentiment de sécurité. Sur ce dernier point, l'étude montre il est vrai que l'installation de caméras de surveillance diminue la peur du crime, mais dans un premier temps seulement, sans qu'il soit pourtant possible d'affirmer avec certitude que cet effet puisse être attribué à la vidéosurveillance. A la suite de l'installation, les habitants des quartiers ainsi surveillés ne croient généralement plus en l'effectivité de tels systèmes [104].

Enfin, il n'est pas certain que les attentats de Londres du 7 juillet 2005 modifient radicalement les conclusions de cette évaluation, dans la mesure où le très dense réseau de vidéosurveillance urbain n'a eu aucun effet dissuasif sur les terroristes, l'utilité du système se révélant plutôt dans la poursuite des infractions.

4.4.2. Les atouts de l'évaluation et de la démarche expérimentale

La question est dès lors de savoir si le degré d'incertitude qui plane sur les effets concrets de la vidéosurveillance est tel que les collectivités publiques ne pourraient même pas tenter l'expérience ou si, malgré cette incertitude, il faut leur reconnaître le droit d'installer et de mettre en œuvre de tels systèmes, quitte à y renoncer si les effets souhaités ne se réalisent pas. Si le choix du système et de ses modalités est le résultat d'un processus démocratique - ce qu'exige la condition de la base légale - il faut sans doute donner la préférence au deuxième terme de cette alternative. Les collectivités publiques sont en droit de choisir en principe les moyens qui leur paraissent les plus appropriés pour atteindre les buts dont la réalisation leur incombe. Pourvu que ce choix émane du législateur, il convient de leur attribuer tout le respect découlant du principe démocratique, et ce respect a pour effet d'atténuer la rigueur de la règle de l'aptitude. Celle-ci n'exige pas que l'efficacité de la mesure envisagée soit dûment prouvée, études empiriques et statistiques à l'appui. Il suffit en général qu'elle ne soit pas exclue d'emblée, qu'elle relève du domaine du possible, sinon du probable. Ainsi, lorsque l'évaluation de l'aptitude dépend de connaissances techniques controversées, ou repose sur des hypothèses, le Tribunal fédéral ne conclut à une violation de la proportionnalité que si elle est manifeste [105].

**** AJP/PJA 2006 page 937 ****

Le droit public a développé différents mécanismes d'aide à la décision dans des situations d'incertitude. L'un d'entre eux est l'autorisation soumise à la condition de réaliser une *évaluation* et de décider de la poursuite de l'expérience en fonction des résultats de celle-ci. Une autre voie possible est l'adoption d'une *base légale expérimentale* dont les effets sont soumis à évaluation afin de décider en connaissance de cause à l'issue de l'expérience.

Sur le plan fédéral, l'obligation de procéder à l'évaluation pour s'assurer de l'efficacité des mesures prises par la Confédération est prévue par la Constitution (art. 170 Cst.) [106]. La révision de la loi sur la protection des données du 24 mars 2006 contient une nouvelle réglementation habilitant le Conseil fédéral à autoriser, avant l'entrée en vigueur d'une loi au sens formel, le traitement automatisé de données sensibles ou de profils de la personnalité dans le cadre d'essais pilotes pour un délai maximal de cinq ans à partir de la mise en œuvre des essais [107].

Sur le plan cantonal, Genève a instauré une Commission externe d'évaluation des politiques publiques [108]. La loi concernant la législation expérimentale du 14 décembre 1995 fixe les conditions qu'une loi doit satisfaire pour être établie à titre expérimental [109].

Confrontées à des problèmes de sécurité à certains endroits du domaine public et du patrimoine administratif accessible à tous, les collectivités publiques doivent pouvoir tenter l'expérience de la vidéosurveillance, même si ses effets réels sont incertains, pour autant que l'essai soit soumis à une procédure d'évaluation sérieuse et indépendante (définition du type de données à récolter, de la démarche méthodologique, des critères d'appréciation et des organes compétents notamment). La Confédération et les cantons devraient adapter leurs bases légales en ce sens.

Les évaluations menées en matière de vidéosurveillance n'ont malheureusement pas toujours été conduites avec la rigueur et l'indépendance nécessaires. Le problème méthodologique demeure complexe il est vrai. Le choix des indicateurs de succès en révèle toute la complication. Si le taux de criminalité est, apparemment, le critère idéal pour déterminer l'efficacité de la vidéosurveillance, il est en vérité peu satisfaisant, dans la mesure où, paradoxalement, son accroissement démontre parfois un succès. La vidéosurveillance a également des effets positifs, non directement voulus, et non mesurables immédiatement en termes de lutte contre les infractions et d'augmentation du sentiment de sécurité, à l'instar de la recherche des enfants égarés [110].

4.4.3. La règle de la nécessité

Toute aussi délicate est la réponse à la question de savoir si la vidéosurveillance constitue le seul moyen

propre à atteindre les buts visés ou si d'autres procédés, moins restrictifs par rapport aux libertés en cause, et possiblement plus économiques, permettent d'arriver aux mêmes fins.

Le principe de la vidéosurveillance mise en place et exploitée par la collectivité publique ne peut pas, à notre avis, être condamné abstraitement en application de la règle de la nécessité. L'on peut certes soutenir que d'autres solutions permettraient d'atteindre le même but, tout en préservant mieux les libertés en cause: présence accrue d'agents de sécurité, en particulier dans les heures creuses (police, contrôleurs ou "*modèles d'accompagnement innovateurs*" comme dans l'exemple des transports publics [111)], éclairage public amélioré des rues ou des places publiques, systèmes d'alarme, mesures architecturales, campagnes de prévention. [112] La vidéosurveillance simple, sans enregistrement ni traitement numérique, doit également être mentionnée dans ce cadre [113], même si elle est probablement en voie de disparition. Mais ces solutions alternatives sont, elles aussi, relativement abstraites et doivent être évaluées à leur tour. Il faut ainsi comparer le degré d'atteinte aux libertés que représenterait une présence policière constante avec celui d'une vidéosurveillance. La première n'est pas négligeable si on la compare avec une surveillance vidéo qui ne se déroule pas en temps réel et dont les données ne sont consultées qu'en cas de problème.

Le problème méthodologique survient lorsque les autres mesures visant au même but sont mises en place parallèlement à la vidéosurveillance [114] . Dans ce cas, il n'est plus possible de déterminer correctement la causalité des mesures instaurées. Ainsi, pour tenir compte de la règle de la

---

nécessité, il faudrait soit d'abord tester la vidéosurveillance indépendamment des autres moyens, soit tester d'autres mesures moins incisives envers les libertés, évaluer leur efficacité, puis les compléter si nécessaire par des dispositifs de vidéosurveillance.

Si l'objectif visé est atteint, c'est-à-dire si la zone surveillée est devenue plus sûre, cela ne signifie pas que les caméras doivent forcément être démontées si l'évaluation montre que leur effet préventif est durable et qu'elles sont la cause immédiate de la sécurité retrouvée. Elles ne devront l'être que si l'évaluation montre l'inverse. Dans toutes les hypothèses, le principe de proportionnalité s'oppose à une vidéosurveillance généralisée de tout le territoire sans tenir compte du niveau d'insécurité qui y règne. Pour être proportionnée, la vidéosurveillance ne peut être installée qu'aux endroits où elle s'avère nécessaire, c'est-à-dire dans les lieux où l'intérêt public visé ne parvient pas à être atteint par d'autres moyens, même si cette limitation accroît le risque de déplacement du vandalisme [115]. Concrètement, la vidéosurveillance doit se limiter aux endroits où, selon l'expérience, se déroulent plus fréquemment des actes de vandalisme et dans lesquels règne par conséquent un plus grand sentiment d'insécurité ("*hotspot*").

Le coût des différentes mesures envisageables peut être un élément à aborder pour juger du respect de la règle de la nécessité. Le Tribunal fédéral a ainsi jugé que si, pour être efficace, une mesure moins grave entraîne des coûts excessifs, l'autorité peut en choisir une plus grave sans violer le principe de proportionnalité [116]. Ainsi, si une mesure plus grave est considérablement moins onéreuse pour la collectivité publique, il n'est pas exclu que l'autorité puisse la retenir au regard de la règle de la nécessité. La différence de coût doit être notable, car des soucis de simple commodité administrative ou des dépenses supplémentaires de faible importance ne justifient pas une restriction à une liberté [117]. En droit allemand, instaurer une vidéosurveillance dans le seul objectif d'économiser les coûts liés aux forces de l'ordre n'est en revanche pas admissible [118].

Or, l'évaluation de l'efficience de la mesure (son rapport coût/bénéfice) n'est pas concluante selon le rapport du Département de l'intérieur anglais [119]. Les coûts sont généralement plus élevés que l'on s'y attend, car ils doivent comprendre l'exploitation des données. Même une vidéosurveillance sans contrôle en temps réel depuis une salle dédiée, limitée à un enregistrement des données, nécessite des ressources en personnel qui peuvent s'avérer importantes dès lors que les personnes exercent leur droit d'accès. Tel est le cas lorsque les passagers surveillés des transports publics s'adressent à la compagnie de transport pour tenter de retrouver les pickpockets. La tâche est d'autant plus difficile que les wagons sont bondés. Dans ce cas, la vidéosurveillance " *devient difficile à exploiter*" [120] .

Le problème principal réside dans la manière de calculer les coûts. L'évaluation anglaise justifie ses conclusions en montrant que là où les résultats ont été les plus prometteurs (en l'espèce dans un parking), l'efficience est faible en raison du coût relativement bas des infractions évitées (déprédation ou vol de véhicules) [121]. Lorsque le coût de réparation des actes de vandalisme est assez faible, la vidéosurveillance

---

ne se justifierait en principe pas sous l'angle de l'efficience. Mais la disproportion ne permet pas sans autre de conclure à la violation de la règle de la nécessité: la détérioration de la sécurité publique entraîne un coût social et politique supérieur, très difficile à exprimer en unités monétaires.

Quoi qu'il en soit, toute réflexion sous l'angle de la règle de la nécessité s'avère hypothétique et donc incertaine, tant il est vrai que l'évaluation et la comparaison des solutions envisageables n'ont de sens que si l'expérience concrète aura permis de vérifier leur efficacité. S'il s'avère que la vidéosurveillance ne donne pas les résultats escomptés, il n'est pas même nécessaire de la comparer à d'autres solutions pour conclure qu'elle est inconstitutionnelle.

4.4.4. La pesée des intérêts

Le dernier test en matière de proportionnalité conduit à une pesée des tous les intérêts en présence: celui de l'Etat à apporter une restriction aux libertés afin d'atteindre les finalités qu'il vise; celui des titulaires de la liberté à ce que l'exercice de celle-ci ne soit pas restreint.

Sous cet angle, la distinction entre la vidéosurveillance avec enregistrement simple et la vidéosurveillance informatisée sous toutes ses formes prend une certaine importance. Rappelons que dans la première, l'atteinte à la vie privée et à la maîtrise informationnelle est certes existante, mais relativement légère. Elle exerce un certain effet préventif, même si celui-ci reste démontrer, et permet de poursuivre une personne surprise par vidéo, soit sur le moment, soit ultérieurement pour autant que celle-ci soit identifiée. L'intérêt public à l'installation et à l'exploitation d'un pareil système de vidéosurveillance limité l'emporte donc sur les inconvénients que ce système comporte pour l'exercice des libertés en cause.

Dans la vidéosurveillance informatisée en revanche, l'atteinte aux libertés se renforce au point de devenir lourde, voire très lourde. Car qui dit numérisation, enregistrement des données personnelles ou couplage biométrique, dit

---

conservation, traitement, profilage, communication de ces données à des tiers et ces opérations comportent toujours, même si elles sont réglementées, un risque non négligeable d'abus. Le danger est particulièrement aigu en raison de l'aisance avec laquelle les données numériques peuvent être aujourd'hui transférées et manipulées [122]. C'est surtout le droit à l'autodétermination informationnelle au sens de l'article 13 al. 2 Cst. qui est lourdement mis à contribution.

Certaines finalités d'intérêt public, qu'il ne s'agit pas d'évaluer dans ce cadre, peuvent paraître limitées au regard de l'atteinte à la sphère privée, à l'instar d'une caméra dont le but serait d'identifier les propriétaires de chien qui ne ramasseraient pas les déjections ou qui ne tiendraient pas leur animal en laisse par exemple, si ces comportements devaient être pénalement répréhensibles. La surveillance d'une déchetterie ou d'un tunnel souterrain pour les piétons est discutable sous cet angle également [123]. Il en va de même du contrôle du respect de l'interdiction de fumer dans certaines zones.

Il faut également tenir compte dans la pesée des intérêts de la capacité d'utiliser la vidéosurveillance dans la poursuite d'infractions [124] .

Dans le domaine de la vidéosurveillance dissuasive des lieux publics ou accessibles à tous, effectuée par des collectivités publiques - ou par des particuliers -, les preuves obtenues en violation des différents principes applicables à ce type de surveillance ne sont admissibles qu'aux conditions très restrictives applicables aux preuves illégales [125] . Tel sera par exemple le sort d'un enregistrement utilisé en violation du principe de finalité, effectué sans indication de l'existence d'une installation, de données conservées audelà de leur durée maximale de conservation ou violant la sphère privée ou le domaine secret des individus (art. 179^{quater} CP).

En revanche lorsque les informations obtenues l'ont été en respect de toutes les règles applicables à la vidéosurveillance dissuasive, elles peuvent en principe être utilisées pour la poursuite d'infractions. La jurisprudence allemande l'admet tant en procédure pénale [126] que civile [127] .

Les seules limites se trouvent dans l'interdiction du visionnement systématique, généralisé et non "personnalisé" des enregistrements effectués, sans qu'il n'existe aucun indice de commission d'une infraction (*Rasterfahndung*, *fishing expedition* [128)]. A supposer que les moyens personnels ou techniques à

---

disposition la rendent possible, une surveillance indirecte, successive et généralisée de toutes les personnes observées s'avère dans cette hypothèse d'emblée incompatible avec le respect des libertés en cause. La police même judiciaire ne peut pas se servir de tels enregistrements pour détecter des infractions, pour "aller à la pêche" aux éventuels fauteurs de trouble [129]. Pour certains auteurs du moins, c'est seulement lorsqu'une enquête pénale a été ouverte, lorsqu'un délit, relativement grave, a été commis et découvert par d'autres moyens, que le recours à l'enregistrement se justifie pour renforcer cette enquête et pour étayer les preuves [130]. Cet auteur fonde son opinion par analogie avec l'interdiction de la "pêche" aux éventuels malfaiteurs relative aux écoutes téléphoniques [131]. La situation en matière de vidéosurveillance dissuasive est pourtant différente dans la mesure où les communications téléphoniques sont soumises au principe du secret, alors que les individus sont filmés en toute transparence dans l'hypothèse de la vidéosurveillance dissuasive.

Le nœud du problème se trouve dans la nécessité ou non de disposer d'un indice pour procéder à l'examen des

---

enregistrements: afin de ne pas être soupçonnée de procéder à une "pêche" aux malfrats, la police ne serait-elle autorisée à procéder aux visionnements uniquement en présence d'un indice, si faible soit-il? Ou, au contraire, ne serait-ce pas précisément la tâche des autorités que de visionner systématiquement les enregistrements, indépendamment de l'existence d'indices concrets, pour vérifier qu'il n'y a pas d'infractions? Dénier aux autorités la compétence de visionner les images sans la présence d'indices remettrait en cause la vidéosurveillance directe en temps réel depuis une salle de contrôle - avec ou sans enregistrement - puisque dans ce cas, tout est, et doit être, systématiquement observé, qu'il y ait un indice ou non.

Les limites se trouvent à notre avis dans le principe de finalité: les bandes ne devraient pas être visionnées pour des motifs autres que ceux pour lesquels la vidéosurveillance est autorisée, par voyeurisme par exemple. Cependant, si une infraction devait être fortuitement découverte à cette occasion, il sera en pratique difficile de prouver une telle motivation.

Un autre problème pratique réside dans le constat d'infractions poursuivies sur plainte uniquement. Dans ce cas, les informations sont inexploitables tant qu'aucune plainte n'est déposée. En matière de vol par exemple, il ne serait pas possible de présumer que les pickpockets agissant dans les transports publics volent des sommes supérieures à la limite qui ne leur permet plus de se soustraire à une poursuite d'office et d'ouvrir ainsi une procédure à défaut de plainte. La situation serait probablement différente dans le cas de la surveillance d'une échoppe de luxe.

En résumé, pour savoir si la découverte d'une infraction par le moyen d'une surveillance par vidéo effectué en violation des règles applicables à la vidéosurveillance peut permettre de poursuivre l'auteur ainsi identifié, il convient de mettre en balance la gravité des infractions qu'il s'agit de poursuivre et l'importance du bien juridique mis en cause par ce moyen de preuve. Le maintien de la sécurité, de la tranquillité et de l'ordre public constitue certes un objectif important. Mais il ne peut justifier l'emploi de tout moyen.

En revanche, lorsque la vidéosurveillance a été effectuée de manière licite, elle peut servir à prouver même des infractions mineures pour autant que celles-ci entrent dans le champ des buts visés par la vidéosurveillance (respect du principe de finalité). Ainsi un vol de quelques dizaines de francs seulement pourra-t-il être prouvé sur la base d'un enregistrement effectué dans les transports publics, alors que tel ne sera pas le cas du propriétaire de chien qui laisse son animal souiller une place publique si la vidéosurveillance n'avait été autorisée que pour des motifs de sécurité.

4.4.5. Les précautions

Dans toutes les hypothèses, certaines précautions s'imposent pour que l'atteinte aux libertés ne soit pas disproportionnée. Ainsi, il est indispensable de veiller, au besoin par des moyens techniques de blocage, à ce que les caméras vidéo ne puissent pas être dirigées contre des immeubles ou des maisons privées sis à proximité des lieux sensibles où le regard indiscret ou distrait de l'observateur risquerait de porter une atteinte en tous points inadmissible à la sphère privée ou au domaine secret (art. 179^{quater} CP) des habitants [132]. L'ordonnance sur la vidéosurveillance des Chemins de fer fédéraux le prévoit expressément, sans que l'on sache exactement comment cette règle peut être effectivement mise en œuvre en pratique.

S'y ajoute que l'enregistrement des données et leur traitement successif nécessitent une réglementation détaillée et des réserves multiples afin d'être compatibles avec la protection de la sphère privée [133]. Il faut déterminer les personnes habilitées à traiter les données, définir et sécuriser le lieu de conservation, fixer un délai maximum de conservation des données personnelles, définir les instances auxquelles les données peuvent être communiquées, informer les personnes que les données les concernant seront enregistrées, réglementer le droit d'accès de ces personnes, leur garantir le droit de consulter les enregistrements en prévoyant d'avance des moyens techniques de cryptage permettant de rendre les autres personnes éventuellement coenregistrées non identifiables. Il faut également prévoir des procédures administratives, et judiciaires, pour que leurs droits soient sauvegardés, en particulier une procédure d'autorisation, ainsi que des procédures de contrôle sur les conditions de fonctionnement des dispositifs autorisés.

Il faut en outre informer les personnes entrant dans la zone surveillée de la présence de caméras. A ce propos, dans le domaine du *droit privé*, l'atteinte aux droits de la personnalité que constitue la vidéosurveillance n'est en principe licite que si elle est justifiée par le consentement de la victime, par un intérêt public ou privé ou par la loi (art. 13 al. 1er LPD). Comme il n'est pas possible de recueillir au préalable le consentement de tous les clients dans un magasin ou de tous les usagers d'un parking, la garantie de la transparence se substitue en quelque sorte à l'impossible consentement. On admet sans autre que, dans ce contexte, les personnes concernées doivent être dûment informées et averties du principe et des modalités de la surveillance, sans doute dans l'idée que si elles devaient s'y opposer, il leur suffirait d'aller faire leurs emplettes ou garer leur véhicule ailleurs. C'est ainsi que l'on pose comme condition que les caméras ne soient pas dissimulées au regard [134], mais mises en évidence et qu'un "*avis lisible*" annonce au public l'existence d'une vidéosurveillance [135].

En *droit public*, pareille précaution peut être discutée. Si la vidéosurveillance n'est pas informatisée et qu'elle

---

s'interdit tout enregistrement des données personnelles, elle peut être exercée de plein droit, sans qu'il soit nécessaire de prévoir des mesures supplémentaires d'information des personnes visées. Après tout, il n'y a pas de panneaux annonçant qu'un agent de la police surveille un site déterminé. Ce n'est que dans l'hypothèse où la collectivité publique estime indispensable de procéder, ponctuellement et à certains endroits bien précis, à l'enregistrement et au traitement des données récoltées que les personnes concernées doivent en être informées. Cette obligation s'explique alors par la nécessité, découlant de l'article 13 al. 2 Cst. et plus précisément de l'article 8 LPD, de garantir le droit d'accès aux données personnelles. Cette exigence découle également des principes directeurs pour la protection des personnes par rapport à la collecte et au traitement de données au moyen de la vidéo-surveillance du Conseil de l'Europe [136], en application du principe de loyauté.

L'exigence d'information découlera pour le surplus de la révision de la LPD du 24 mars 2006 dont l'article 4 al. 4 exige le caractère reconnaissable de la collecte. Celui-ci pose le principe selon lequel la collecte doit être reconnaissable pour la personne concernée, notamment ses finalités, complété à l'article 7a par un devoir d'information plus détaillé pour les données personnelles sensibles et les profils de la personnalité [137].

Il faudra donc préciser les conditions d'information du public sur l'existence du dispositif de vidéosurveillance ainsi que sur l'identité de la personne responsable (information claire et permanente sur le lieu surveillé). De façon générale, l'information doit également porter sur l'existence du droit d'accès des personnes filmées aux enregistrements les concernant et de leur droit de saisir les instances compétentes pour faire respecter leurs droits. La vidéosurveillance par avions télécommandés (drones) pose dans ce contexte un problème particulier. Pour autant qu'un tel procédé soit admissible (ce qui devrait s'avérer douteux sous l'angle de la proportionnalité), il serait nécessaire d'informer par divers moyens que telle région est surveillée électroniquement depuis le ciel.

Afin d'éviter sur le plan fédéral une prolifération de réglementations diverses comme l'exposé des législations spéciales le montre, il serait grand temps de réviser la LPD sur ce point en proposant une base légale formelle générale, explicite et uniforme pour la vidéosurveillance dissuasive tant des lieux publics et accessibles à tous ressortissant à la compétence fédérale que des lieux privés accessibles à tous. Contrairement aux lois actuellement en vigueur ou en projet, la base dans la LPD devrait être plus précise. Un traitement différencié des endroits ouverts au public selon que ceux-ci sont en mains publiques ou privées ne trouve aucune justification du point de vue de l'utilisateur. Les cantons devront également rattraper leur retard en adaptant en conséquence leurs lois sur la protection des données dans le cadre de

---

leurs compétences.

Dans tous les cas de figure, il faudra prendre en compte le caractère expérimental en limitant dans le temps les autorisations et en prévoyant la réalisation d'évaluations indépendantes.

5. Conclusions

La vidéosurveillance consistant à surveiller ouvertement le domaine public et le patrimoine administratif librement accessible au public afin de prévenir la commission d'infractions (vidéosurveillance dissuasive) *n'est pas d'emblée inconstitutionnelle*.

Dans la mesure où il faut considérer d'une manière générale que les données personnelles ainsi recueillies sont des données sensibles, une *base légale formelle expresse* est exigée lorsque les organes fédéraux les traitent. En droit cantonal, la base légale dépend des exigences posées pour le traitement des données sensibles ainsi que du *degré d'atteinte aux libertés*. Celui-ci dépend de l'agencement du dispositif:

-- une *vidéosurveillance non informatisée* permettant d'identifier des personnes sans enregistrement ne porte en principe pas atteinte aux libertés, sauf dans des circonstances particulières, par exemple si elle est permanente et individualisée;

-- une *vidéosurveillance avec enregistrement simple*, effacé automatiquement après une brève durée, constitue une atteinte légère; l'atteinte est plus intrusive si l'enregistrement est doublé d'un suivi en temps réel en salle de contrôle ou s'il est en haute résolution, doté de caméras orientables et réglables à distance;

-- une *vidéosurveillance avec traitement informatisé*, permettant d'établir des profils de personnalité en couplage ou non avec des bases de données biométriques, de suivre automatiquement une scène, d'initier des alarmes en fonction de l'analyse de comportements types ou de caractéristiques prédéfinies constitue une atteinte grave; atteinte plus intrusive encore si l'on recourt à Internet pour communiquer les données ou les visualiser, accroissant le risque de leur diffusion incontrôlée.

Le critère de *l'intérêt public* est rempli si le but visé est de prévenir des infractions pénales. Lutter contre des "incivilités" n'est pas suffisant pour justifier une atteinte aux libertés.

Les études scientifiques récentes laissent planer un doute sur l'efficacité réelle de la vidéosurveillance. Dès lors, afin de satisfaire à la *règle de l'aptitude* dans l'examen de la proportionnalité, la vidéosurveillance ne saurait être autorisée qu'à la condition de soumettre l'expérience à une procédure d'évaluation sérieuse et indépendante. Pour satisfaire à la

---

règle de la nécessité, la surveillance par vidéo doit se limiter aux endroits où, selon l'expérience, se déroulent plus fréquemment des actes de vandalisme et dans lesquels règne un plus grand sentiment d'insécurité. Enfin, sous l'angle de la *pesée des intérêts*, toutes les finalités d'intérêt public ne justifient pas nécessairement l'atteinte aux libertés que cause la vidéosurveillance. Dans toutes les hypothèses, un certain nombre de précautions supplémentaires s'imposent pour que la vidéosurveillance respecte le principe de la proportionnalité: respect du domaine secret, anonymisation, procédure d'autorisation, cercle des personnes habilitées, information du public, conservation et communication des données notamment.

Il appartient à la Confédération, aux cantons et aux communes de légiférer, dans le cadre de leurs compétences et avec la précision et les précautions nécessaires, pour que la vidéosurveillance soit consacrée, limitée, voire même proscrite, avec le sceau de la légitimité démocratique que seule la loi peut lui conférer. Et il reviendra au juge de tracer la ligne de partage entre les restrictions admissibles aux libertés, que les particuliers doivent supporter, et celles qui vont au-delà de ce qui est utile et nécessaire, que la Constitution condamne.

En matière de vidéosurveillance, la Constitution peut fermer un œil, si la loi le lui demande, si l'intérêt public l'exige et si la proportionnalité est respectée. Mais elle ne saurait fermer les deux.

Notes de bas de page:

[1] Sur ces notions, voir notamment BRUNO BAERISWYL , "Videoüberwachung: im rechtsfreien Raum? Datenschutzrechtliche Aspekte moderner Überwachung mittels optischen Geräten", DIGMA 2002, p. 27 .

---

[2] Ainsi par exemple, la vidéosurveillance du trafic routier, qui est en principe d'observation, se recouvre toujours davantage avec la vidéosurveillance dissuasive ou invasive, dans la mesure où elle permet d'identifier les propriétaires des véhicules au moyen des plaques minéralogiques; IVO SCHWEGLER, Datenschutz im Polizeiwesen von Bund und Kantonen, Berne, 2001, p. 60; MARKUS MÜLLER/URSULA WYSSMANN, Polizeiliche Videoüberwachung: Rechtssetzungszuständigkeit nach bernischem Polizeigesetz, JAB 2005, p. 542 s.

[3] ATF 6S.358/2004 du 10 novembre 2004, consid. 5.3 et 6.2.

[4] Art. 10 de la loi d'orientation et de programmation relative à la sécurité du 21 janvier 1995, modifiée le 6 août 2004, art. 15. Cette disposition a fait l'objet d'une décision du Conseil constitutionnel du 18 janvier 1995 (no 94-352 DC).

[5] Art. 6b Bundesdatenschutzgesetz du 20 décembre 1990, révisée le 14 janvier 2003 (BGBl. I, p. 66).

[6] RS 235.1

[7] Préposé fédéral à la protection des données, *Aide-mémoire sur la vidéosurveillance effectuée par des personnes privées*, Berne, janvier 2003.

[8] I. SCHWEGLER (n. 2), p. 65 s.

[9] Pour I. SCHWEGLER (n. 2), une base légale matérielle serait même souhaitable, s'agissant de la vidéosurveillance des lieux privés ouverts au public par la police, p. 65 s.

[10] MICHEL HOTTELIER, "La réglementation du domaine public à Genève", SJ 2002 II 123 , 124, 126; PIERRE MOOR, Droit administratif, vol. III, Berne 1992, p. 253 ss, 321 ss; ANDRÉ GRISEL, Traité de droit administratif, vol. II Neuchâtel 1984, p. 525 ss.

[11] Rappelons qu'il n'existe pas de domaine public fédéral, P. MOOR (n. 10), p. 257.

[12] RS-GE L 1 05.

[13] A. GRISEL (n. 10), p. 539.

[14] Dans un avis de droit portant sur la licéité de l'installation d'une vidéosurveillance dans un parking souterrain, l'Office fédéral de la justice n'a pas manqué de noter que "*le vandalisme, que l'on veut à juste titre combattre, n'est-il pas plutôt le fait de personnes qui pénètrent à cette fin dans un parking et le plus souvent sans voiture?*"; JAAC 56 no 20, p. 169 s.

[15] FF 1988 II 421, 473.

[16] JEAN-PHILIPPE WALTER, in: *Kommentar zum Bundesgesetz über den Datenschutz*, Bâle/Francfort-sur-le-Main 1995, ad art. 17, no 17.

[17] J.-P. WALTER (n. 16), ad art. 17 no 17.

[18] J.-P. WALTER (n. 16), ad art. 17 no 22.

[19] FF 2006 3421 (délai référendaire: 13 juillet 2006).

[20] FF 2003 1952.

[21] RS 120.72.

[22] RS 120.

[23] Sur la vidéosurveillance invasive, voir en outre l'art. 9 OMSI, ainsi que les art. 279 et 281 du projet de code de procédure pénale suisse du 21 décembre 2005.

[24] RS 631.09.

[25] Délai de 24 heures avant le 1er mars 2005; RO 1994 2471; ch. I de l'ordonnance du 16 février 2005, RO 2005 1101.

[26] RS 631.0.

[27] Le préposé fédéral à la protection des données est d'avis qu'une ordonnance n'est pas suffisante si la conservation des données dépasse quelques jours (Préposé fédéral à la protection des données, *1er rapport d'activités* 1993/1994, chapitre "Autres thèmes", ch. 8).

[28] RS 742.147.2.

[29] B. BAERISWYL, "Entwicklungen im Datenschutzrecht; le point sur le droit de la protection des données", SJZ 2004, p. 460.

[30] Art. 19 al. 1er et 23 de la loi fédérale sur les chemins de fer (RS 742.101).

[31] FF 2005 2439.

[32] L'art. 62 du projet de nouvelle loi fédérale sur le transport de voyageurs (FF 2005 2403) s'applique tant aux voyageurs qu'à l'exploitation.

[33] Commissaires suisses à la protection des données, *Rapport concernant la surveillance vidéo dans les transports publics*, 20 juin 2004, p. 9.

[34] RS 935.521.

[35] Ordonnance sur les systèmes de surveillance et les jeux de hasard le 24 septembre 2004, RS 935.521.21.

[36] RS 935.52.

[37] Les autres cantons sont en train de créer les bases légales nécessaires. Voir par exemple Argovie où le projet de loi du 6 juillet 2005 (*Gesetz über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen*) prévoit à l'article 20 une base légale spécifique réglementant la vidéosurveillance dissuasive en la soumettant à autorisation (al. 1er *i.f.*);

Schwyz: Conseil d'Etat du canton de Schwyz, *Video-Überwachung im Kanton Schwyz: Beantwortung der Motion M 7/05*, 9 août 2005; Vaud: Motion Pierre-André Pidoux et consorts du 25 octobre 2005 demandant au Conseil d'Etat de légiférer sur la mise en place de caméras de surveillance dans les espaces publics, 8 novembre 2005); Berne: réponse du Conseil d'Etat à diverses interventions parlementaires du 8 février 2006; Genève: un projet de loi cantonale sur la protection des données réglementant cette question notamment a été adopté par le conseil d'Etat (Conseil d'Etat, Point presse du 7 juin 2006).

[38] Sur l'application du principe de légalité aux actes étatiques non obligataire, voir ALEXANDRE FLÜCKIGER, "Régulation, dérégulation, autorégulation: l'émergence des actes étatiques non obligatoires", RDS 2004, II, p. 262 ss.

[39] Datenschutzbeauftragter des Kantons Zürich, *Videoüberwachung durch öffentliche Organe: Grundlagen*, juillet 2002; *Empfehlungen und Checkliste* , décembre 2005; Zürcher Verkehrsverbund, *Richtlinien Für Pilotversuche Videoüberwachung im ZVV* , 15 décembre 2003.

[40] Datenschutzbeauftragter Basel-Landschaft, *Merkblatt Videoüberwachung durch Gemeinden*, Liestal, sans date (publié sur Internet le 26 août 2003).

[41] Datenschutzbeauftragter des Kantons Luzern, *Merkblatt zur Videoüberwachung durch Gemeinden und Kanton*, novembre 2003; *Muster-Reglement Videoüberwachung* , février 2006.

[42] Autorité cantonale de surveillance en matière de protection des données, *Surveillance vidéo: aide-mémoire concernant la surveillance vidéo effectuée par des organes publics cantonaux et communaux dans des lieux et bâtiments publics*, avril 2005.

[43] Loi du canton de Bâle-Ville sur la protection des données du 18 mars 1992; RS-BS 153.260.

[44] Modification du 20 octobre 2004.

[45] *Verordnung über die Videoüberwachung* du 4 janvier 2005, RS-BS 153.290.

[46] Loi sur la protection des informations traitées automatiquement par ordinateur du 24 juin 1976, art. 17.

[47] RS-GE B 4 35.

[48] RS-GE B 4 35.01.

[49] PASCALE ERBEIA, *Les citoyens face aux données numériques*, 13e journée de Rencontre-Sphère privée et Protection des données (http://www.geneve.ch/obstech).

[50] Commission externe d'évaluation des politiques publiques du canton de Genève (CEPP), *La communication entre les services de l'administration cantonale: Evaluation de la circulation de l'information dans le cadre de l'attribution de prestations sociales* , Genève 2002, p. 34 ss et 65.

[51] Conseil d'Etat du canton de Genève, Décision du 10 décembre 2003.

[52] Conseil d'Etat du canton de Genève, Décision du 3 novembre 2004, annulant et remplaçant celle du 10 décembre 2003, ch. 5.

[53] On trouve dans d'autres cantons quelques exemples de réglementation communale en la matière; par exemple à Marly dans le canton de Fribourg (art. 20 bis du règlement de police du 18 mars 1987, article approuvé le 5 août 2005 par la Direction de la sécurité et de la justice).

[54] M. MÜLLER/U. WYSSMANN (n. 2). A la suite de cet avis de droit, la commune de Berne a renoncé à édicter un règlement sur la vidéosurveillance (Ville de Berne, communiqué de presse du 17 août 2005).

[55] RS/GE B 6 05.

[56] Voir le règlement concernant l'utilisation du domaine public, du 21 décembre 1988 (RS-GE L 1 10 12), qui ne laisse aux communes qu'une compétence d'exécution, notamment en matière d'autorisations pour usage accru concernant les voies publiques communales.

[57] M. HOTTELIER (n. 10), p. 162: "*les autorités municipales disposent de la compétence de réglementer et d'aménager, sur le terrain pratique, l'utilisation des biens rentrant dans leur domaine public ou leur patrimoine administratif*".

[58] CHRISTIAN M. REISER, *Autonomie et démocratie dans les communes genevoises*, Bâle 1998.

[59] Conseil d'Etat, *Point presse*, 29 mars 2006.

[60] RAINER J. SCHWEIZER, "Verfassungsrechtlicher Persönlichkeitsschutz", in: DANIEL THÜRER/GEORG AUBERT/JEAN-FRANÇOIS MÜLLER (éd.), *Droit constitutionnel suisse*, Zurich 2001 § 43, p. 692; ANDREAS AUER/GIORGIO MALINVERNI/M. HOTTELIER, *Droit constitutionnel suisse* vol. II Les droits fondamentaux, 2e éd. Berne 2006, no 326.

[61] ATF 107 Ia 138 , 145 *P*.

[62] ATF 109 Ia 146 , 155 *Comité contre la loi sur la police*.

[63] ATF 127 I 6, 11 P.; 123 I 112, 118 *Rolf Himmelberger* .

[64] ATF 107 Ia 52, 57 *Z*.

[65] RAINER J. SCHWEIZER, in: *St-Galler Kommentar*, Zurich/Lachen/St.Gallen 2002, art. 10 no 26.

[66] ATF 127 I 6, 12 P.

[67] AUER/MALINVERNI/HOTTELIER (n. 60) no 344.

[68] AUER/MALINVERNI/HOTTELIER (n. 60) no 369; JEAN-FRANÇOIS AUBERT/PASCAL MAHON, *Petit commentaire de la Constitution fédérale de la Confédération Suisse du 18 avril 1999*, Zurich 2003, ad art. 10 no 17.

[69] ATF 109 Ia 146 , 150 *Comité contre la loi sur la police*.

[70] Art. 26 al. 2 de l'ordonnance 3 relative à la loi sur le travail (RS 822.113).

[71] ATF 130 II 425 , 447.

[72] Conseil constitutionnel, Décision no 94-352 DC du 18 janvier 1995 (Loi d'orientation et de programmation relative à la sécurité), ad art. 10; JACQUES GEORGEL, *Les libertés de communication*, Paris, 1996, p. 49. *Contra* en droit allemand, voir DIRK BÜLLESFELD, Polizeiliche *Videoüberwachung öffentlicher Strassen und Plätze zur Kriminalitätsvorsorge* , Stuttgart (etc.), 2002, p. 234 ss.

[73] Commission nationale de l'informatique et des libertés (CNIL), *24e rapport d'activité 2003*, Paris, p. 136.

[74] Dans une affaire relative à l'admissibilité d'un système de géolocalisation d'une flotte de voitures par un employeur, le Tribunal fédéral a estimé que si un tel procédé permettait "*de suivre de manière continue et en temps réel le trajet emprunté par les véhicules utilisés par les techniciens-vérificateurs, il pourrait constituer un moyen de surveillance disproportionné par rapport au but poursuivi*.", ATF 130 II 425 , 447.

[75] AUER/MALINVERNI/HOTTELIER (n. 60) no 384; ATF 124 I 34 36 *B* .

[76] SCHWEIZER 2001 (n. 60), p. 702.

[77] ACEDH *P.G. et J.H. c. Royaume-Uni* du 25 septembre 2001, § 56. Voir ég. l'arrêt *Peck c. Royaume-Uni* (ACEDH du 28 janvier 2003): communiquer aux média pour diffusion le film de la tentative de suicide d'une personne, enregistrée par des caméras de vidéosurveillance, avait été considérée comme une ingérence grave dans la vie privée, alors même que la personne visée se trouvait dans un lieu public au moment des faits.

[78] STEPHAN BREITENMOSER, in: *St.Galler Kommentar*, art. 13 al. 1 no 13.

[79] ACEDH *Botta* du 24 février 1984, Rec. 1998 - I 412 § 32.

[80] ACEDH *Perry c. Royaume-Uni* du 17 juillet 2003, no 38. La Cour se référant en particulier à l'affaire *Herbecq et autre c. Belgique*, décision de la Commission du 14 janvier 1998, DR 92-A, p. 92.

[81] ACEDH *Perry c. Royaume-Uni* du 17 juillet 2003, no 40. L'opinion selon laquelle, dans cette hypothèse, si le droit à l'image n'est pas atteint, la protection de la vie privée et la liberté personnelle l'est en revanche (VANESSA LÉVY, *Le droit à l'image: définition, protection, exploitation*, Zurich 2001, p. 203) ne saurait être suivie telle quelle.

[82] ACEDH *Perry c. Royaume-Uni* du 17 juillet 2003, no 38, se référant aux arrêts *Rotaru c. Roumanie* (GC), no 28341/95, no 43 s, CEDH 2000-V et *Ammann c. Suisse* (GC), no 65 à 67, CEDH 2000-II, où il a été jugé que la collecte de données sur des individus déterminés par les services de sécurité constituait une ingérence dans la vie privée des personnes intéressées, bien que ces données avaient été recueillies sans l'aide de techniques de surveillance secrète.

[83] ATF 129 V 323, 325 *F*; dans le cas d'espèce, l'atteinte était cependant couverte par la loi, justifiée par un intérêt public et proportionnelle; confirmé: TFA, arrêt du 20 mars 2006, *U* 289/05, c. 2.5. Voir aussi un arrêt de la 2ème Cour civile du 18 décembre 1997 SJ 1998 301, confirmé par la Cour européenne des droits de l'homme JAAC 65 (2001) no 134 p. 1381 , qui concernait une vidéosurveillance effectuée par une compagnie d'assurances, considérée en l'espèce comme conforme à l'art. 28 CC.

[84] Dans le contexte de l'admissibilité de l'utilisation de preuves obtenues de manière illicite: "*Zu Recht hat es erwogen, die Tiefgarage sei ein 'quasi-öffentlicher' Raum, in dem sich die Überwachten in der Regel zeitlich eng begrenzt aufhalten. Zwar fand die Überwachung rund um die Uhr statt, die Aufnahmen wurden aber automatisch alle 24 Stunden gelöscht. Unter diesen Umständen kann eine schwere Beeinträchtigung der Persönlichkeitsrechte des Beschwerdeführers verneint werden* ." (ATF 131 I 272 *X* , consid. 6.2 (non publié aux ATF)).

[85] ATF 130 II 425 , 447 s, *X*.

[86] ATF 130 II 425 , 445, *X*.

[87] ATF 109 Ia 146 , 157 *Comité contre la loi sur la police*; ATF 113 I 1, 7 *M*., ATF 113 Ia 257 , 263 *P*.; ATF 120 Ia 147 *B*.; ATF 122 I 360 *B* .; ATF 124 I 34, 36 *B*.; ATF 125 I 257, 260 *J.H*.

[88] SCHWEIZER (n. 60) no 29.

[89] RAINER J. SCHWEIZER, in: *St-Galler Kommentar* art. 13 no 38.

[90] ATF 126 I 7, 10, 12 O.; AUBERT/MAHON (n. 68), ad art. 13 no 16.

[91] Office fédéral de la justice, avis du 29 juillet 1992, JAAC 56 no 20.

[92] L'ordonnance sur la vidéosurveillance CFF du 5 décembre 2003 (RS 742.147.2) prévoit ainsi que ce n'est que "*lorsque les enregistrements contiennent des données personnelles*" que ceux-ci sont analysés puis détruits dans les 24 heures (art. 4 al. 2).

[93] Bâle-Ville, art. 6a de la loi cantonale sur la protection des données du 18 mars 1992; Commission nationale française de l'informatique et des libertés, *Voix, image, et protection des données personnelles*, Paris, 1996, p. 65.

[94] I. SCHWEGLER (n. 2), p. 63. Certains cantons disposent de bases légales spécifiques réglementant la vidéosurveillance par la police durant les manifestations (par exemple GE: art. 22 de la loi sur la police du 26 octobre 1957, RS-GE F 1 05, ou BE: ordonnance sur l'usage par la police d'enregistreurs d'images et de son lors de manifestations de masse du 20 décembre 1989, RS-BE 551.332).

[95] Pour M. MÜLLER/U. WYSSMANN (n. 2), p. 540 note 34, la vidéosurveillance doit toutefois toujours reposer sur une base légale formelle, car il serait incontesté qu'elle porte atteinte aux libertés.

[96] ATF 120 Ia 147 , 151 (traduction).

[97] Sur cette notion, voir BAPTISTE VIREDAZ , *Le sentiment d'insécurité: devons-nous avoir peur?* Grolley 2005.

[98] I. SCHWEGLER (n. 2), p. 58 estime que le renforcement du sentiment de sécurité du public peut justifier une surveillance

par vidéo, mais pas nécessairement l'enregistrement des données personnelles.

[99] JAAC 56 (1992) no 20 p. 165.

[100] Autorité cantonale de surveillance en matière de protection des données, *Surveillance vidéo: aide-mémoire concernant la surveillance vidéo effectuée par des organes publics cantonaux et communaux dans des lieux et bâtiments publics*, avril 2005.

[101] Sur ces notions P. MOOR, Droit administratif, vol. I, 2e éd., Berne 1994, ch. 5.2.1.2; Systématique et illustration du principe de la proportionnalité, in: Mélanges Michel Fromont, Strasbourg 2001, p. 319 ss; AUER/MALINVERNI/HOTTELIER (n. 60) no 226-247.

[102] MARTIN GILL/ANGELA SPRIGGS, *Assessing the impact of CCTV*, Home Office research study 292, Londres, février 2005. En Suisse, voir FRANCISCO KLAUSER, *Die Videoüberwachung als Aneignungsform öffentlicher Räume*, Thèse Fribourg, à paraître, selon lequel la vidéosurveillance n'est ni une solution miracle pour lutter contre la criminalité, ni - prise isolément - une mesure permettant d'améliorer durablement la situation dans les endroits sensibles.

[103] GILL/SPRIGGS 2005 (n. 102), p. 59.

[104] GILL/SPRIGGS 2005 (n. 102), p. 57 et 60.

[105] ZBl 1991 25, 31 pour la fluorisation de l'eau potable; ATF 119 Ia 197 , 209 à propos de l'interdiction du canoë sur des rivières dans lesquelles des espèces animales sont en voie de disparition. Sur la détermination du seuil minimum en matière de connaissance scientifique, ALEXANDRE FLÜCKIGER , La preuve juridique à l'épreuve du principe de précaution, Revue européenne des sciences sociales, 2003, p. 107 ss, 116 s.

[106] ALEXANDRE FLÜCKIGER, Le droit administratif en mutation: l'émergence d'un principe d'efficacité, Revue de droit administratif et fiscal, 2001, p. 93-119.

[107] Art. 17a nLPD; FF 2006 3421 (délai référendaire: 13 juillet 2006).

[108] Loi sur la surveillance de la gestion administrative et financière et l'évaluation des politiques publiques du 19 janvier 1995; RS-GE D 1 10.

[109] RS-GE A 2 35; pour une description détaillée, voir ALEXANDRE FLÜCKIGER, Voter, élire et signer par Internet: le droit expérimental à l'épreuve de la sécurité, in: HANNA MURALT MÜLLER/ANDREAS AUER/THOMAS KOLLER (éd.), *E-voting*, Berne, 2003, p. 107 ss, 112 ss.

[110] GILL/SPRIGGS 2005 (n. 102), p. 117.

[111] "Grands frères", accompagnement des élèves et parrainage des gares (CFF, Rapport de gestion 2004, Berne, p. 35).

[112] Pour un aperçu de quelques mesures possibles à titre alternatif, voir BARBARA MATHIS AEPPLI, "Checkliste zur Videoüberwachung", DIGMA 2003, p. 22 s.

[113] Il faut relever, sur le plan de la prévention d'infractions et du renforcement du sentiment subjectif de sécurité des individus, que l'enregistrement n'est pas *a priori* plus efficace que la surveillance simple I. SCHWEGLER (n. 2), p. 60.

[114] Tel a par exemple été le cas des CFF qui, pour lutter contre l'augmentation de l'agressivité et du vandalisme ont instauré une nouvelle stratégie de sécurité combinant des méthodes de prévention et d'intervention dans les gares et les trains en prévoyant l'application de mesures techniques (vidéosurveillance en particulier) et le recours à des ressources humaines (augmentation des effectifs de la police ferroviaire de 52 unités, modèles d'accompagnements innovateurs, etc.) (CFF, *Rapport de gestion 2004*, Berne, p. 34).

[115] GILL/SPRIGGS 2005 (n. 102) p. 72.

[116] P. MOOR (n. 101) p. 410 se référant aux ATF 103 Ia 594 , *Jacquemin* et ATF 101 Ia 336 , 342, *Automatenbranche* , à propos des difficultés administratives d'un contrôle répressif.

[117] ATF 114 Ia 1, *X* . Sur cette question, voir P. MOOR (n. 101), ch. 5.1.4.

[118] STEPHAN BAUSCH, Videoüberwachung als präventives Mittel der Kriminalitätsbekämpfung in Deutschland und in Frankreich, Marburg, 2004, p. 58 ss; DIRK BÜLLESFELD (n. 72), p. 62, note 29.

[119] "*CCTV cannot be deemed a success. It has cost a lot of money and it has not produced the anticipated benefits*", GILL/SPRIGGS 2005 (n. 102) p. 120.

[120] Tribune de Genève, édition du 8 décembre 2005, p. 21.

[121] GILL/SPRIGGS 2005 (n. 102), p. 114.

[122] GILL/SPRIGGS 2005 p. 120.

[123] Dans le même sens, voir Aide-mémoire fribourgeois 2005 (n. 42), ch. 4.2 let. a.

[124] Sur l'utilisation des enregistrements vidéo par les autorités policières et judiciaires, voir I. SCHWEGLER, Digitale Fotografie bei Polizei und Justiz: Chancen und Risiken aus rechtlicher Sicht, AJP/ *PJA* 2004, p. 657 ss, 663 ss (les propos de l'auteur relatifs à l'utilisation des photographies digitales s'appliquent par analogie aux enregistrements vidéo).

[125] Les preuves illégales ne peuvent être exploitées qu'après une pesée d'intérêts (MARKUS SCHEFER, *Grundrechte in der Schweiz*, Berne, 2005, p. 139 s). Une affaire récente l'illustre. Le Tribunal fédéral a jugé en 2005 (ATF 131 I 272, *X*.) que la vidéosurveillance par la police d'un garage souterrain dont le dispositif efface automatiquement les enregistrements après 24 heures, dans le cadre d'une enquête devait être considérée comme une preuve illégale dans la mesure où l'autorisation préalable n'avait pas été demandée au juge compétent. Ce cas est à considérer comme un exemple de vidéosurveillance invasive puisque la police tentait de traquer un incendiaire dans cette affaire. Il ne préjuge pas de la question de l'utilisation par la police du matériel qui aurait été enregistré par le propriétaire d'un parking privé dans le contexte d'une vidéosurveillance dissuasive ordinaire. La surveillance par vidéo des parkings par leur propriétaire n'est en soi pas prohibée pour autant que le droit civil relatif à la protection de la personnalité et la législation sur la protection des

données concernant les personnes privées soit respectées (Préposé fédéral à la protection des données 2003 (n. 7); *contra*: Office fédéral de la justice, avis de droit du 29 juillet 1992, JAAC 56 (1992) no 20 p. 169).Sur la base du droit privé (art. 28 CC), le Tribunal fédéral a jugé cependant en 1997 qu'une société d'assurance était autorisée à faire suivre secrètement par un détective privé au moyen d'enregistrements vidéo une femme soupçonnée de simuler certaines atteintes corporelles (Tribunal fédéral, arrêt 5C.187/1997 du 18 décembre 1997 (cité ci-dessus note 83); voir ég. ATF 129 V 323 U et les critiques (MARCO FEY, "Schweizerisches Bundesgericht; Urteil U 16/01 vom 25. Februar 2003", DIGMA 2003, p. 130 , 131)); TFA, Arrêt du 20 mars 2006, U 289/05, c. 2.5.

[126] NJW 2002, 2893 (vidéosurveillance dans un grand magasin clairement indiquée à l'entrée de celui-ci).

[127] MARTIN W. HUFF, "Videoüberwachung im öffentlichen und privaten Bereich: eine Zwischenbilanz", JuS 10/2005, p. 896 ss, 899.

[128] I. SCHWEGLER (n. 2), p. 137 s; SCHEFER 2005 (n. 125), p. 139.

[129] SCHEFER (n. 125), p. 139.

[130] I. SCHWEGLER (n. 2), p. 61.

[131] I. SCHWEGLER (n. 2), note de bas de page 78, p. 61.

[132] ATF 118 IV 41, 50 *F*.

[133] On trouvera une liste dans BARBARA MATHIS AEPPLI, "Checkliste zur Videoüberwachung", DIGMA 2003, p. 23 s ou dans les directives cantonales notamment.

[134] JAAC 56 (1992) no 20 p. 169.

[135] Préposé fédéral à la protection des données 2003 (n. 7).

[136] Conseil de l'Europe, *Rapport contenant des principes directeurs pour la protection des personnes par rapport à la collecte et au traitement de données au moyen de la vidéo-surveillance (2003)*, adopté par le Comité européen de Coopération juridique (CDCJ) lors de sa 78e réunion, 20-23 mai 2003.

[137] FF 2006 3421 (délai référendaire: 13 juillet 2006).

Liste d'autorité

Lois citées:

0-101	Conv. du 4 novembre 1950 de sauvegarde des droits de l'homme et des libertés fondamentales (CEDH)
Art. 8	
Art. 19	
101	Constitution fédérale de la Confédération suisse du 18 avril 1999 (Cst.)
Art. 5	
Art. 10	
Art. 13	
Art. 22	
Art. 36	
Art. 164	
Art. 170	
120	LF du 21 mars 1997 instituant des mesures visant au maintien de la sûreté intérieure (LMSI)
120-2	O du 27 juin 2001 sur les mesures visant au maintien de la sûreté intérieure (OMSI)
Art. 9	
120-72	O du 27 juin 2001 sur la sécurité relevant de la compétence fédérale (OSB)
Art. 15	
210	Code civil suisse du 10 décembre 1907 (CC)
Art. 28	
235-1	LF du 19 juin 1992 sur la protection des données (LPD)
Art. 3	
Art. 4	
Art. 8	
Art. 13	
Art. 17	
311-0	Code pénal suisse du 21 décembre 1937 (CP)
Art. 179quater	
631-0	LF du 1er octobre 1925 sur les douanes (LD)
631-09	O du 26 octobre 1994 réglant la surveillance de la frontière verte au moyen d'appareils vidéo
742-101	LF du 20 décembre 1957 sur les chemins de fer (LCdF)
Art. 62	
742-147-2	O du 5 décembre 2003 sur la vidéosurveillance des Chemins de fer fédéraux (CFF) (Ordonnance sur la vidéosurveillance CFF, OVsur-CFF)
822-113	O 3 du 18 août 1993 relative à la loi sur le travail (Hygiène, OLT 3)
935-52	LF du 5 octobre 1929 sur les maisons de jeu
Art. 14	

935-521	O du 23 février 2000 sur les jeux de hasard et les maisons de jeu (Ordonnance sur les maisons de jeu, OLMJ)
935-521-21	O du DFJP du 13 mars 2000 sur les systèmes de surveillance et les jeux de hasard (Ordonnance sur les jeux de hasard, OJH)

Arrêts cités:

AJP-2004-657_667	Digitale Fotografie bei Polizei und Justiz - Chancen und Risiken aus rechtlicher Sicht
AZA-U.16/01	U.16/01 Urteil vom 24. Juli 2001.
AZA-U.289/05	U.289/05 Urteil vom 20. März 2006.
BGE-101-IA-336_348	59. Auszug aus dem Urteil vom 24. September 1975 i.S. Verband der Schweizerischen Automatenbranche und Mitbeteiligte gegen Kanton Basel-Landschaft
BGE-103-IA-594_602	87. Auszug aus dem Urteil vom 13. Dezember 1977 i.S. Jacquemin gegen Einwohnergemeinde Bern und Verwaltungsgericht des Kantons Bern
BGE-107-IA-138_148	27. Auszug aus dem Urteil der I. öffentlichrechtlichen Abteilung vom 3. Juni 1981 i.S. P. und Mitbeteiligte gegen Untersuchungs- und Polizeiorgane ...
BGE-107-IA-52_59	11. Auszug aus dem Urteil der I. öffentlichrechtlichen Abteilung vom 28. Januar 1981 i.S. Z. gegen Betreibungsamt Olten-Gösgen und Aufsichtsbehörde ...
BGE-109-IA-146_159	27. Extrait de l'arrêt de la Ire Cour de droit public du 6 juillet 1983 dans la cause Comité contre la loi sur la police et Duvanel contre Grand ...
BGE-113-IA-257_266	41. Extrait de l'arrêt de la Ire Cour de droit public du 3 juin 1987 dans la cause P. contre Président de la Chambre d'accusation et Chef de la ...
BGE-114-IA-1_7	1. Auszug aus dem Urteil der II. öffentlichrechtlichen Abteilung vom 22. Januar 1988 i.S. X. gegen Ausgleichskasse Schweizer Wirteverband (Aarau) und ...
BGE-118-IV-41_51	10. Urteil des Kassationshofes vom 24. Januar 1992 i.S. F. gegen Staatsanwaltschaft des Kantons Basel-Landschaft und H. (Nichtigkeitsbeschwerde)
BGE-119-IA-197_213	24. Auszug aus dem Urteil der II. öffentlichrechtlichen Abteilung vom 7. Mai 1993 i.S. Schweizerischer Kanuverband, Kanu Klub Bern, Paddel Club Bern, ...
BGE-120-IA-147_156	21. Auszug aus dem Urteil der I. öffentlichrechtlichen Abteilung vom 15. Juni 1994 i.S. B. gegen Staatsanwaltschaft des Kantons Basel-Stadt ...
BGE-122-I-360_369	45. Auszug aus dem Urteil der I. öffentlichrechtlichen Abteilung vom 28. November 1996 i.S. B. und Mitbeteiligte gegen Regierungsrat des Kantons ...
BGE-123-I-112_143	13. Arrêt de la Ire Cour de droit public du 16 avril 1997 dans la cause Rolf Himmelberger contre Grand Conseil du canton de Genève (recours de droit ...
BGE-124-I-34_39	5. Auszug aus dem Urteil der I. öffentlichrechtlichen Abteilung vom 30. Januar 1998 i.S. B. gegen N., Bezirksanwaltschaft Zürich und ...
BGE-125-I-257_267	24. Extrait de l'arrêt de la Ie Cour de droit public du 24 juin 1999 dans la cause J.H. contre Président du Tribunal cantonal du canton de Vaud ...
BGE-126-I-7_14	2. Extrait de l'arrêt de la Ière Cour de droit public du 23 mars 2000 dans la cause O. contre Chambre d'accusation et Chef de la police du canton de ...
BGE-127-I-6_30	2. Auszug aus dem Urteil der I. öffentlichrechtlichen Abteilung vom 22. März 2001 i.S. P. gegen Psychiatrische Universitätsklinik Basel und ...

BGE-129-V-323_326	48. Auszug aus dem Urteil i.S. F. gegen Schweizerische Unfallversicherungsanstalt und Versicherungsgericht des Kantons Aargau U 161/01 vom 25. ...
BGE-130-II-425_448	38. Extrait de l'arrêt de la IIe Cour de droit public dans la cause X. SA contre Office cantonal de l'inspection et des relations du travail ainsi ...
BGE-131-I-272_283	29. Auszug aus dem Urteil der I. öffentlichrechtlichen Abteilung i.S. X. gegen Staatsanwaltschaft sowie Kantonsgericht Basel-Landschaft ...
BVR-2005-529_554	Polizeiliche Videoüberwachung Rechtssetzungszuständigkeit nach bernischem Polizeigesetz
DIGMA-2002-26_28	Videoüberwachung - im rechtsfreien Raum? Datenschutzrechtliche Aspekte moderner Überwachung mittels optischen Geräten
DIGMA-2003-130_131	Schweizerisches Bundesgericht; Urteil U 16/01 vom 25. Februar 2003; http://www.bger.ch über Rechtsprechung I Urteile ab 2000
DIGMA-2003-22_24	Checkliste zur Videoüberwachung
RDAF-2001-I-93_119	Le droit administratif en mutation: l'émergence d'un principe d'efficacité
SJ-1998-301_304	Audience du 18 décembre 1997. -- C.V. c. Secura Compagnie d'assurances
SJ-2002-II-123_175	LA REGLEMENTATION DU DOMAINE PUBLIC À GENEVE
SJZ-100-460_463	Entwicklungen im Datenschutzrecht/Le point sur le droit de la protection des données
VPB-56-20	20. Office fédéral de la justice, avis du 25 juin 1991, mis à jour le 29 juillet 1992.
VPB-65-134	134. Déc. de la Cour eur. DH du 28 juin 2001, déclarant irrecevable la req. N° 41953/98, présentée par Catherine VERLIERE c/Suisse
ZBL-1991-25_33	Bundesgericht, II. Öffentlichrechtliche Abteilung, 29. Juni 1990.